

WEIGHTED GENERATING FUNCTIONS FOR TYPE II LATTICES AND CODES

NOAM D. ELKIES AND SCOTT DUKE KOMINERS

ABSTRACT. We give a new structural development of harmonic polynomials on Hamming space, and harmonic weight enumerators of binary linear codes, that parallels one approach to harmonic polynomials on Euclidean space and weighted theta functions of Euclidean lattices. Namely, we use the finite-dimensional representation theory of \mathfrak{sl}_2 to derive a decomposition theorem for the spaces of discrete homogeneous polynomials in terms of the spaces of discrete harmonic polynomials, and prove a generalized MacWilliams identity for harmonic weight enumerators. We then present several applications of harmonic weight enumerators, corresponding to some uses of weighted theta functions: an equivalent characterization of t -designs, the Assmus–Mattson Theorem in the case of extremal Type II codes, and configuration results for extremal Type II codes of lengths 8, 24, 32, 48, 56, 72, and 96.

1. INTRODUCTION

A well-known and fruitful analogy relates lattices L in Euclidean space \mathbb{R}^n with linear codes C in binary Hamming space \mathbb{F}_2^n . (See for instance [Ebe02], [Elk00], and [CS99, 3.2].) Under this analogy the theta function

$$(1.1) \quad \Theta_L(q) = \sum_{v \in L} q^{\langle v, v \rangle / 2} = \sum_{k \geq 0} \left(\sum_{\langle v, v \rangle = 2k} 1 \right) q^k,$$

a generating function that counts vectors $v \in L$ in spheres $\{v : \langle v, v \rangle = 2k\}$ about the origin, corresponds to the weight enumerator

$$(1.2) \quad W_C(x, y) = \sum_{c \in C} x^{n - \text{wt}(c)} y^{\text{wt}(c)} = \sum_{w=0}^n \left(\sum_{\text{wt}(c)=w} 1 \right) x^{n-w} y^w,$$

a generating function that counts words $c \in C$ in Hamming spheres $\{c : \text{wt}(c) = w\}$ about the origin. This paper concerns a generalization of Θ_L and W_C that can be used not only to count lattice or code elements in each sphere, by summing the constant function 1 as in (1.1) and (1.2), but also to measure their distribution, by summing a suitable nonconstant function P . In the

2000 *Mathematics Subject Classification.* Primary: 94B05; Secondary: 05B05, 11H71, 33C50, 33C55.

Key words and phrases. Harmonic polynomial, weight enumerator, binary code, extremal code, theta function, lattice, design, configuration result.

The authors thank Zachary Abel, Henry Cohn, John H. Conway, John F. Duncan, Benedict H. Gross, Abhinav Kumar, Barry Mazur, Gabriele Nebe, Ken Ono, Vera Pless, Eric M. Rains, and Shrenik Shah for helpful comments and suggestions. During parts of this research, Elkies was supported by NSF grants DMS-0501029 and DMS-1100511, and Kominers was supported by the Harvard College Program for Research in Science and Engineering (PRISE), a Harvard Mathematics Department Highbridge Fellowship, an NSF Graduate Research Fellowship, a Yahoo! Key Scientific Challenges Program Fellowship, and an AMS-Simons Travel Grant.

This work includes a part of the second author's undergraduate thesis [Kom09b].

lattice case, P is a harmonic polynomial on \mathbb{R}^n , yielding the weighted theta function

$$(1.3) \quad \Theta_{L,P}(q) = \sum_{v \in L} P(v) q^{\langle v, v \rangle / 2} = \sum_{k \geq 0} \left(\sum_{\langle v, v \rangle = 2k} P(v) \right) q^k.$$

In the code case, P is a discrete harmonic polynomial on \mathbb{F}_2^n , yielding the harmonic weight enumerator¹

$$(1.4) \quad W_{C,P}(x, y) = \sum_{c \in C} P(c) x^{n - \text{wt}(c)} y^{\text{wt}(c)} = \sum_{w=0}^n \left(\sum_{\text{wt}(c)=w} P(c) \right) x^{n-w} y^w.$$

Weighted theta functions have been used extensively to study the configurations of lattice vectors. But discrete harmonic polynomials and harmonic weight enumerators are relatively unknown and rarely used. Moreover, the known construction of discrete harmonic polynomials P , and the known proofs of the basic properties of these P and of the associated $W_{C,P}$ (see [Del78, Bac99]), involve manipulations of intricate combinatorial sums that are considerably harder than, and look nothing like, the developments of their Euclidean counterparts.

Here we give a structural development of discrete harmonic polynomials and harmonic weight enumerators that parallels the more familiar theory of harmonic polynomials on \mathbb{R}^n and weighted theta functions. In each case we use an action of the Lie algebra \mathfrak{sl}_2 on spaces of functions on \mathbb{R}^n (for lattices) or on \mathbb{F}_2^n (for codes). While the two cases are not completely parallel, the remaining distinctions are inherent in the structure of Euclidean and Hamming space; for instance, homogeneous polynomials on \mathbb{F}_2^n cannot be defined by $P(cv) = c^d P(v)$, and since Hamming space is finite all the representations of \mathfrak{sl}_2 that figure in the discrete theory are finite-dimensional. Once we have established the new approach to discrete harmonic polynomials and harmonic weight enumerators, we use it to give cleaner derivations of the Assmus–Mattson theorem [AM69] and the Koch condition [Koc87] on the tetrad system of a Type II code of length 24.² Finally we outline some further applications to the configurations of minimal-weight words in extremal Type II codes that parallel recent configuration results for extremal Type II lattices.

The rest of the paper is organized as follows. We first outline the \mathfrak{sl}_2 approach to harmonic polynomials on \mathbb{R}^n and to the construction and basic properties of weighted theta functions, and the connection with design properties of Type II lattices. In the next section we review the MacWilliams identity for weight enumerators and Gleason’s theorem for the weight enumerator of a Type II code. In the following three sections we use the \mathfrak{sl}_2 theory to develop the theory of discrete harmonic polynomials P , prove the MacWilliams identity for harmonic weight enumerators $W_{C,P}$, and study the important special case where P is a “zonal harmonic polynomial” (discrete harmonic polynomial invariant under a subgroup $S_w \times S_{n-w}$ of the group S_n of coordinate permutations of \mathbb{F}_2^n). The next two sections relate these polynomials with t -designs and recover the Assmus–Mattson theorem for extremal Type II codes and the Koch condition for Type II codes of length 24. Finally we use these techniques to show for several values of n that any extremal Type II code of length n is generated by its words of minimal weight, again in analogy with known results for extremal Type II lattices. In an Appendix, we give a direct

¹ While the analogy between $\Theta_{L,P}$ and $W_{C,P}$ suggests calling $W_{C,P}$ a “weighted weight enumerator”, the comical juxtaposition of the two senses of “weight” dissuades us from using that phrase. Since Bachoc [Bac99] had already introduced the term “harmonic weight enumerator” that avoids this juxtaposition, we happily follow her usage.

² The second of these requires only the $W_{C,P}$ for P of degree 1, which coincide with Ott’s “local weight enumerators” [Ott99].

proof of Gleason's theorems for self-dual codes of Type I and II; certain polynomials needed to describe harmonic weight enumerators occur naturally in the course of this proof.

While the present paper considers codes only over \mathbb{F}_2 , discrete harmonic polynomials and harmonic weight enumerators generalize to linear codes over arbitrary finite fields \mathbb{F}_q (see [Bac01]). Our development of these notions extends to that setting too, using representations of \mathfrak{sl}_q instead of \mathfrak{sl}_2 . This change introduces enough new complications that we defer the analysis to a separate paper.

2. WEIGHTED THETA FUNCTIONS AND CONFIGURATIONS OF TYPE II LATTICES

2.1. Lattice-Theoretic Preliminaries. By a *lattice* in Euclidean space \mathbb{R}^n we mean a discrete subgroup $L \subset \mathbb{R}^n$ of rank n ; equivalently, L is the \mathbb{Z} -span of the columns of an invertible $n \times n$ real matrix, say M (which does not depend uniquely on L : two such matrices M, M' yield the same L iff $M^{-1}M'$ has integer entries and determinant ± 1). The *covolume* $\text{Vol}(\mathbb{R}^n/L)$ of the lattice is then $|\det M|$. The *dual lattice* is defined by

$$(2.1) \quad L^* = \{v^* \in \mathbb{R}^n : \forall v \in L, \langle v, v^* \rangle \in \mathbb{Z}\}.$$

If L is the \mathbb{Z} -span of the columns of the invertible matrix M then L^* is the \mathbb{Z} -span of the columns of the transpose of M^{-1} ; in particular $\text{Vol}(\mathbb{R}^n/L^*) = \text{Vol}(\mathbb{R}^n/L)^{-1}$.

If $L = L^*$ then L is *self-dual*. Then $\langle v, v' \rangle \in \mathbb{Z}$ for all $v, v' \in L$, and the norm map $L \rightarrow \mathbb{Z}$, $v \mapsto \langle v, v \rangle$ reduces modulo 2 to a group homomorphism $L \rightarrow \mathbb{Z}/2\mathbb{Z}$. The lattice is said to be *even* or *of Type II* if this homomorphism is trivial, that is, if $\langle v, v \rangle \in 2\mathbb{Z}$ for all $v \in L$; otherwise L is said to be *odd* or *of Type I*.

Examples. For each $n \geq 1$ the lattice $\mathbb{Z}^n \subset \mathbb{R}^n$ is of Type I. It is the unique Type I lattice in \mathbb{R}^n for $n = 1$, and unique up to isomorphism for $n \leq 8$, but not unique for any $n \geq 9$; there are finitely many isomorphism classes of Type I lattices in \mathbb{R}^n , but the number of classes grows rapidly with n (see for instance [CS99, p. 403]).

If \mathbb{R}^n contains a Type II lattice then $n \equiv 0 \pmod{8}$ (see [Ser73, Chapter V]). Such a lattice may be constructed as follows. For any n let D_n be the sublattice of \mathbb{Z}^n consisting of all (x_1, \dots, x_n) such that $\sum_{j=1}^n x_j \equiv 0 \pmod{2}$, and let D_n^+ be the union of D_n and the translate of D_n by the half-integer vector $(1/2, 1/2, \dots, 1/2)$. Then D_n^+ is:

- a lattice if and only if $2 \mid n$,
- self-dual if and only if $4 \mid n$, and
- of Type II if and only if $8 \mid n$.

For $n = 8$, this lattice D_8^+ coincides with the Gosset root lattice E_8 , which is known to be the unique Type II lattice in \mathbb{R}^8 up to isomorphism; we give one proof of its uniqueness at the end of this section.³ There are two Type II lattices for $n = 16$ (namely $E_8 \oplus E_8$ and D_{16}^+), and 24 for $n = 24$ (the Niemeier lattices [Nie73]); for large $n \equiv 0 \pmod{8}$ the number is again always finite but grows rapidly as $n \rightarrow \infty$ (see for instance [CS99, p. 50]).

2.2. Poisson Summation. The *Poisson summation formula* is a remarkable identity relating the sum of a function f over a lattice and the sum of the Fourier transform of f over the dual lattice. We review this formula in the case of Schwartz functions, which is all that we need. Recall that a *Schwartz function* is a C^∞ function $f : \mathbb{R}^n \rightarrow \mathbb{C}$ such that f and all its

³ Serre [Ser73, Chapter VII] uses the notation E_n for our D_n^+ for all $n \equiv 0 \pmod{8}$, but this notation has not been widely adopted. For $n \equiv 4 \pmod{8}$ the Type I lattice D_n^+ is isomorphic with \mathbb{Z}^n if and only if $n = 4$.

partial derivatives decay as $o(\langle x, x \rangle^k)$ for all k as $\langle x, x \rangle \rightarrow \infty$. We define the *Fourier transform* $\hat{f} : \mathbb{R}^n \rightarrow \mathbb{C}$ by

$$(2.2) \quad \hat{f}(y) = \int_{x \in \mathbb{R}^n} f(x) e^{2\pi i \langle x, y \rangle} d\mu(x);$$

\hat{f} is a Schwartz function if f is.

Theorem 2.1 (Poisson Summation Formula). *Let L be any lattice in \mathbb{R}^n . Then*

$$(2.3) \quad \sum_{x \in L} f(x) = \frac{1}{\text{Vol}(\mathbb{R}^n/L)} \sum_{y \in L^*} \hat{f}(y)$$

for all Schwartz functions $f : \mathbb{R}^n \rightarrow \mathbb{C}$.

Proof. Define $F : \mathbb{R}^n \rightarrow \mathbb{C}$ by

$$F(z) = \sum_{x \in L} f(x + z).$$

Because f is Schwartz, the sum converges absolutely to a C^∞ function, whose value at $z = 0$ is the left-hand side of (2.3). Since $F(z) = F(x + z)$ for all $z \in \mathbb{R}^n$ and $x \in L$, the function descends to a C^∞ function on \mathbb{R}^n/L , and thus has a Fourier expansion

$$(2.4) \quad F(z) = \sum_{y \in L^*} \hat{F}(-y) e^{2\pi i \langle y, z \rangle},$$

where

$$\hat{F}(y) = \frac{1}{\text{Vol}(\mathbb{R}^n/L)} \int_{z \in \mathbb{R}^n/L} F(z) e^{2\pi i \langle y, z \rangle} d\mu(z).$$

Note that the vectors $y \in L^*$ are exactly those for which $e^{2\pi i \langle x, y \rangle}$ is well-defined on \mathbb{R}^n/L . Now choose a fundamental domain R for \mathbb{R}^n/L ; for instance, let v_1, \dots, v_n be generators of L and set $R = \{a_1 v_1 + \dots + a_n v_n : 0 \leq a_i < 1\}$. Then we have

$$\begin{aligned} \text{Vol}(\mathbb{R}^n/L) \hat{F}(y) &= \int_{z \in R} F(z) e^{2\pi i \langle y, z \rangle} d\mu(z) \\ &= \int_{z \in R} \sum_{x \in L} f(x + z) e^{2\pi i \langle y, z \rangle} d\mu(z) \\ &= \sum_{x \in L} \int_{z \in R+x} f(z) e^{2\pi i \langle y, z \rangle} d\mu(z) \\ &= \int_{z \in \mathbb{R}^n} f(z) e^{2\pi i \langle y, z \rangle} d\mu(z) = \hat{f}(y), \end{aligned}$$

where we used in the last step the fact that \mathbb{R}^n is the disjoint union of the translates $R + x$ of R by lattice vectors. Thus (2.4) becomes

$$(2.5) \quad F(z) = \frac{1}{\text{Vol}(\mathbb{R}^n/L)} \sum_{y \in L^*} \hat{f}(-y) e^{2\pi i \langle y, z \rangle}.$$

Taking $z = 0$ we obtain (2.3). □

2.3. Theta Functions. Suppose now that q is a real number with $0 < q < 1$. We may then take $f(x) = q^{\langle x, x \rangle / 2}$ and recognize the left-hand side of (2.3) as the sum $\Theta_L(q)$ of (1.1). The Poisson summation formula then yields the following functional equation for theta functions.

Proposition 2.2. *Let L be any lattice in \mathbb{R}^n . Then*

$$(2.6) \quad \Theta_{L^*}(e^{-2\pi t}) = \text{Vol}(\mathbb{R}^n/L) t^{-n/2} \Theta_L(e^{-2\pi/t})$$

for all $t > 0$.

Proof. Let $f(x) = \exp(-\pi \langle x, x \rangle / t)$ in (2.3). We claim that

$$(2.7) \quad \hat{f}(y) = t^{n/2} \exp(-\pi \langle y, y \rangle t).$$

Indeed, choosing any orthonormal coordinates (x_1, \dots, x_n) for \mathbb{R}^n , we see that the integral (2.2) defining $\hat{f}(y)$ factors as

$$\prod_{j=1}^n \int_{-\infty}^{\infty} e^{-\pi x_j^2 / t} e^{2\pi i x_j y_j} dx_j,$$

which reduces our claim to the case $n = 1$, which is the familiar definite integral

$$\int_{-\infty}^{\infty} e^{-\pi x^2 / t} e^{2\pi i x y} dx = t^{1/2} e^{-\pi t y^2}$$

(see for instance [Rud76, Example 9.43, pp. 237–238] or [Kör90, Lemma 50.2(i), pp. 246–247]). Using these f and \hat{f} in the Poisson summation formula (2.3) we deduce the functional equation (2.6). \square

Now suppose L is a Type II lattice. Then $L^* = L$, so the functional equation relates Θ_L to itself, and $\text{Vol}(\mathbb{R}^n/L) = 1$. Moreover, each of the exponents $\langle v, v \rangle / 2$ occurring in the formula (1.1) is an integer, so $\Theta_L(q)$ is a power series in q and extends to a function on the unit disc $|q| < 1$ in \mathbb{C} . Thus by analytic continuation the identity $\Theta_L(e^{-2\pi t}) = t^{-n/2} \Theta_L(e^{-2\pi/t})$ holds for all $t \in \mathbb{C}$ of positive real part. But $\Theta_L(e^{-2\pi t})$, being a power series in $e^{-2\pi t}$, is also invariant under $t \mapsto t + i$. This leads us to define the function

$$(2.8) \quad \theta_L(\tau) := \Theta_L(e^{2\pi i \tau}) = \sum_{v \in L} e^{\pi \langle v, v \rangle i \tau}$$

for τ in the Poincaré upper half-plane

$$\mathcal{H} := \{\tau \in \mathbb{C} : \text{Im}(\tau) > 0\}.$$

Then $\theta_L(\tau) = \theta_L(\tau + 1)$, and the Poisson identity gives $\theta_L(\tau) = t^{-n/2} \theta_L(-1/\tau)$: the expected factor of $i^{n/2}$ disappears because $n \equiv 0 \pmod{8}$ for all Type II lattices. It follows that

$$(2.9) \quad \theta_L(\tau) = (c\tau + d)^{-n/2} \theta_L\left(\frac{a\tau + b}{c\tau + d}\right)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in the subgroup of $\text{SL}_2(\mathbb{R})$ generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. This subgroup is the full modular group $\text{SL}_2(\mathbb{Z})$ of integer matrices of determinant 1. (See [Ser73, Chapter VII] for this and the remaining results noted in this paragraph.) The identity (2.9) for all such $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, together with the fact that $\theta_L(\tau)$ remains bounded as $\text{Im}(\tau) \rightarrow \infty$ (because then $q \rightarrow 0$), then shows that θ_L is a modular form of weight $n/2$ for $\text{SL}_2(\mathbb{Z})$. Since $n/2 \equiv 0 \pmod{4}$, this means that θ_L is a polynomial in the normalized Eisenstein series

$$\mathcal{E}_4 = \theta_{E_8}(\tau) = 1 + 240 \sum_{n=1}^{\infty} \frac{n^3 q^n}{1 - q^n} = 1 + 240q + 2160q^2 + 6720q^3 + \dots$$

of weight 4 (where again $q = e^{2\pi i\tau}$) and the cusp form⁴

$$\Delta(\tau) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = q - 24q^2 + 252q^3 - 1472q^4 \dots$$

of weight 12. Moreover the coefficient of $\mathcal{E}_4^{n/8}$ in this polynomial equals 1 because that coefficient is the constant coefficient in the q -expansion, which is the number of lattice vectors of norm zero.

It follows for example that if $n = 8$ or $n = 16$ then $\theta_L = \mathcal{E}_4^{n/8}$, while if $n = 8m$ with $m = 3, 4$, or 5 and L contains no vectors v with $\langle v, v \rangle = 2$ then $\theta_L = \mathcal{E}_4^m - 240m\theta_{E_8}^{m-3}\Delta$ (so for example the q^2 coefficient is $720m(211 - 40m) > 0$ and L has that many vectors v with $\langle v, v \rangle = 4$). It is known that such L are unique up to isomorphism for $n = 8$ and $n = 24$ (the E_8 and Leech lattices respectively), but there are two choices for $n = 16$, and literally millions for $n = 32$ (see [Kin03]) and many more for $n = 40$, all with the same number of vectors of norm $2k$ for each k .

More generally, given any $n = 8m$ the theta series of any Type II lattice L can be written uniquely as $\mathcal{E}_4^m + \sum_{k=1}^{\lfloor m/3 \rfloor} a_k \Delta^k \mathcal{E}_4^{m-3k}$ for some a_k . If L contains no vectors v with $0 < \langle v, v \rangle \leq 2\lfloor m/3 \rfloor$ then the a_k are uniquely determined by induction, and thus all such lattices have the same theta series. Such lattices L are known as *extremal lattices*, and their common theta function θ_L is the *extremal theta function*. Siegel [Sie69] proved that the $q^{\lfloor m/3 \rfloor + 1}$ coefficient of θ_L is positive, from which Mallows, Odlyzko, and Sloane [MOS75] deduced that a Type II lattice $L \subset \mathbb{R}^n$ has minimal norm at most $2(\lfloor m/3 \rfloor + 1)$, with equality if and only if L is extremal.

2.4. The Spaces of Harmonic Polynomials. Let \mathcal{P} be the \mathbb{C} -vector space of polynomials on \mathbb{R}^n , and \mathcal{P}_d ($d = 0, 1, 2, \dots$) its subspace of homogeneous polynomials of degree d , so that $\mathcal{P} = \bigoplus_{d=0}^{\infty} \mathcal{P}_d$. The *Laplacian* is the differential operator defined by⁵

$$(2.10) \quad \Delta = \sum_{j=1}^n \frac{\partial^2}{\partial x_j^2} : C^\infty(\mathbb{R}^n) \rightarrow C^\infty(\mathbb{R}^n), \quad \mathcal{P} \rightarrow \mathcal{P}, \quad \mathcal{P}_d \rightarrow \mathcal{P}_{d-2}.$$

Here x_1, \dots, x_n are any orthonormal coordinates on \mathbb{R}^n , and \mathcal{P}_d is taken to be $\{0\}$ for $d < 0$. The space of *harmonic polynomials* of degree d is then

$$(2.11) \quad \mathcal{P}_d^0 := \ker(\Delta : \mathcal{P}_d \rightarrow \mathcal{P}_{d-2});$$

this is the degree- d homogeneous part of

$$(2.12) \quad \mathcal{P}^0 := \bigoplus_{d=0}^{\infty} \mathcal{P}_d^0 = \ker(\Delta : \mathcal{P} \rightarrow \mathcal{P}).$$

For example, \mathcal{P}_0^0 and \mathcal{P}_1^0 are the spaces of constant and linear functions respectively, of dimensions 1 and n ; and a quadratic polynomial $P = \sum_{1 \leq j \leq k \leq n} a_{jk} x_j x_k$ is harmonic if and only if $\sum_{j=1}^n a_{jj} = 0$, because ΔP is the constant polynomial $2 \sum_{j=1}^n a_{jj}$.

⁴ That is, a modular form vanishing at all the cusps; for $\mathrm{SL}_2(\mathbb{Z})$ there is only one cusp, at $\mathrm{Im}(\tau) \rightarrow \infty$, so a modular form in $\mathrm{SL}_2(\mathbb{Z})$ is a cusp form if and only if its expansion as a power series in q has constant coefficient zero. Note that the notation of [Ser73] diverges from the usual practice that we follow: our \mathcal{E}_4 , \mathcal{E}_6 , and Δ are what Serre calls E_2 , E_3 and $(2\pi)^{-12}\Delta$. (We use “ \mathcal{E} ” rather than “ E ” to avoid confusion with the E_8 lattice.)

⁵ The use of Δ for this operator and Δ for the modular form $\eta^{24} = q \prod_{n=1}^{\infty} (1 - q^n)^{24}$ may be unfortunate, but should not cause confusion, despite the similarity between the two symbols, because they never appear together outside this footnote. The alternative notation L for the Laplacian would be much worse, as we regularly use L for a lattice.

It is well known, and we shall soon demonstrate, that $\Delta : \mathcal{P}_d \rightarrow \mathcal{P}_{d-2}$ is surjective, whence

$$(2.13) \quad \dim(\mathcal{P}_d^0) = \dim(\mathcal{P}_d) - \dim(\mathcal{P}_{d-2}) = \binom{n+d-1}{d} - \binom{n+d-3}{d}.$$

We shall use two further operators on $C^\infty(\mathbb{R}^n)$ and on its subspace \mathcal{P} . The first is

$$(2.14) \quad \mathbf{E} := x \cdot \nabla = \sum_{j=1}^n x_j \frac{\partial}{\partial x_j}.$$

Euler proved that if $P \in C^\infty(\mathbb{R}^n)$ is homogeneous of degree d then $\mathbf{E}P = d \cdot P$; in particular \mathcal{P}_d is the d -eigenspace of $\mathbf{E}|_{\mathcal{P}}$. The second operator is multiplication by the norm:

$$(2.15) \quad \mathbf{F} := \langle x, x \rangle = \sum_{j=1}^n x_j^2 : P \mapsto \langle x, x \rangle P.$$

Clearly \mathbf{F} injects each \mathcal{P}_d into \mathcal{P}_{d+2} . Thus $\mathcal{P}_d^0 = \ker(\mathbf{F}\Delta : \mathcal{P}_d \rightarrow \mathcal{P}_d)$; that is, \mathcal{P}_d^0 is the zero eigenspace of the operator $\mathbf{F}\Delta$ on \mathcal{P}_d . We next show that the other eigenspaces are $\mathbf{F}^k \mathcal{P}_{d-2k}^0$ for $k = 1, 2, \dots, \lfloor d/2 \rfloor$, and that \mathcal{P}_d is the direct sum of these eigenspaces, from which the surjectivity of $\Delta : \mathcal{P}_d \rightarrow \mathcal{P}_{d-2}$ will follow as a corollary.

We begin with by finding the commutators of $\Delta, \mathbf{E}, \mathbf{F}$. Recall that the *commutator* of any two operators A, B on some vector space is

$$[A, B] = AB - BA = -[B, A].$$

For example, $[x_j, x_k] = [\partial/\partial x_j, \partial/\partial x_k] = 0$ for all j, k , while $[\partial/\partial x_j, x_k] = \delta_{jk}$ (Kronecker delta). Applying these formulas repeatedly, we obtain the commutation relations

$$(2.16) \quad [\Delta, \mathbf{F}] = 4\mathbf{E} + 2n, \quad [\mathbf{E}, \Delta] = -2\Delta, \quad [\mathbf{E}, \mathbf{F}] = 2\mathbf{F}.$$

This suggests the commutation relations

$$(2.17) \quad [\mathbf{X}, \mathbf{Y}] = \mathbf{H}, \quad [\mathbf{H}, \mathbf{X}] = 2\mathbf{X}, \quad [\mathbf{H}, \mathbf{Y}] = -2\mathbf{Y}$$

satisfied by the standard basis

$$(2.18) \quad (\mathbf{X}, \mathbf{H}, \mathbf{Y}) = \left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right)$$

of \mathfrak{sl}_2 . Indeed (2.16) is tantamount to an isomorphism of Lie algebras from \mathfrak{sl}_2 to the span of $\{\Delta, \mathbf{E} + \frac{n}{2}, \mathbf{F}\}$ that takes $(\mathbf{X}, \mathbf{H}, \mathbf{Y})$ to $(\frac{1}{2\varpi}\Delta, -(\mathbf{E} + \frac{n}{2}), -\frac{\varpi}{2}\mathbf{F})$ for some nonzero ϖ (all choices of ϖ are equivalent via conjugation by diagonal matrices; later the choice $\varpi = 2\pi$ will be most natural for us). Some steps in the following analysis are familiar from the representation theory of \mathfrak{sl}_2 , though here only infinite-dimensional representations arise.

Now suppose $P \in \mathcal{P}_d$ is in the λ -eigenspace of $\mathbf{F}\Delta$ for some λ . Then $\langle x, x \rangle P = \mathbf{F}P$ is in the $(\lambda + 4d + 2n)$ -eigenspace of $\mathbf{F}\Delta$ acting on \mathcal{P}_{d+2} , because

$$\mathbf{F}\Delta \mathbf{F}P = \mathbf{F}(\mathbf{F}\Delta + [\Delta, \mathbf{F}])P = \mathbf{F}(\mathbf{F}\Delta + 4\mathbf{E} + 2n)P = \mathbf{F}(\lambda + 4d + 2n)P.$$

By induction on $k = 0, 1, 2, \dots$ it follows that $\mathbf{F}^k P$ is an eigenvector of $\mathbf{F}\Delta|_{\mathcal{P}_{d+2k}}$ with eigenvalue

$$\lambda + \sum_{j=0}^{k-1} 4(d + 2j) + 2n = \lambda + k(4(d + k - 1) + 2n).$$

Replacing d by $d - 2k$ and taking $\lambda = 0$, we see that if $P \in \mathcal{P}_{d-2k}^0$ then $\mathbf{F}^k P$ is an eigenvector of $\mathbf{F}\Delta|_{\mathcal{P}_d}$ with eigenvalue

$$\lambda_d(k) := k(4(d - k - 1) + 2n).$$

We next prove that this accounts for all the eigenspaces of $\mathbf{F}\Delta|_{\mathcal{P}_d}$.

Lemma 2.3. *Fix $d \geq 0$. For integers k, k' such that $0 \leq k < k' \leq d/2$ we have $\lambda_d(k) < \lambda_d(k')$.*

Proof. By induction it is enough to check this for $k' = k + 1$. We compute

$$\lambda_d(k+1) - \lambda_d(k) = 2n + 4(d - 2k') \geq 2n > 0,$$

as claimed. \square

Corollary 2.4. *The sum of the subspaces $\mathbf{F}^k \mathcal{P}_{d-2k}^0$ of \mathcal{P}_d over $k = 0, 1, \dots, \lfloor d/2 \rfloor$ is direct.*

Proof. By Lemma 2.3, the $\lambda_d(k)$ are strictly increasing, and thus distinct. Our claim follows because $\mathbf{F}^k \mathcal{P}_{d-2k}^0$ is a subspace of the $\lambda_d(k)$ eigenspace of $\mathbf{F}\Delta$. \square

Proposition 2.5. *For $k = 0, 1, \dots, \lfloor d/2 \rfloor$, let $\mathcal{P}_d^k = \mathbf{F}^k \mathcal{P}_{d-2k}^0$. Then:*

- (1) *The map $\Delta : \mathcal{P}_d \rightarrow \mathcal{P}_{d-2}$ is surjective.*
- (2) *$\mathcal{P}_d = \bigoplus_{k=0}^{\lfloor d/2 \rfloor} \mathcal{P}_d^k = \mathcal{P}_d^0 \oplus \mathbf{F}\mathcal{P}_{d-2}$, and $\mathcal{P} = \bigoplus_{k=0}^{\infty} \mathbf{F}^k \mathcal{P}^0$.*
- (3) *\mathcal{P}_d^k is the entire $\lambda_d(k)$ eigenspace of $\mathbf{F}\Delta|_{\mathcal{P}_d}$, and $\mathbf{F}\Delta|_{\mathcal{P}_d}$ has no eigenvalues other than the $\lambda_d(k)$ for $k = 0, 1, \dots, \lfloor d/2 \rfloor$.*
- (4) *$\dim(\mathcal{P}_d^0) = \dim(\mathcal{P}_d) - \dim(\mathcal{P}_{d-2})$ as claimed in (2.13).*

Proof. The sum $\bigoplus_{k=0}^{\lfloor d/2 \rfloor} \mathcal{P}_d^k$ is direct by Corollary 2.4. We prove that it equals \mathcal{P}_d by comparing dimensions. Since \mathbf{F} is injective we have $\dim(\mathcal{P}_d^k) = \dim(\mathcal{P}_{d-2k}^0)$; moreover

$$\dim(\mathcal{P}_{d-2k}^0) \geq \dim(\mathcal{P}_{d-2k}) - \dim(\mathcal{P}_{d-2k-2}),$$

with equality if and only if $\Delta : \mathcal{P}_{d-2k} \rightarrow \mathcal{P}_{d-2k-2}$ is surjective, because \mathcal{P}_{d-2k}^0 is the kernel of $\Delta : \mathcal{P}_{d-2k} \rightarrow \mathcal{P}_{d-2k-2}$. Hence $\dim(\bigoplus_{k=0}^{\lfloor d/2 \rfloor} \mathcal{P}_d^k)$ is

$$(2.19) \quad \sum_{k=0}^{\lfloor d/2 \rfloor} \dim(\mathcal{P}_d^k) = \sum_{k=0}^{\lfloor d/2 \rfloor} \dim(\mathcal{P}_{d-2k}^0) \geq \sum_{k=0}^{\lfloor d/2 \rfloor} (\dim(\mathcal{P}_{d-2k}) - \dim(\mathcal{P}_{d-2k-2})),$$

and the last sum telescopes to $\dim(\mathcal{P}_d)$. Thus equality holds termwise in the last step of (2.19) and $\dim(\bigoplus_{k=0}^{\lfloor d/2 \rfloor} \mathcal{P}_d^k) = \dim(\mathcal{P}_d)$. The first of these proves part (1) (using the $k = 0$ term). The second yields

$$(2.20) \quad \mathcal{P}_d = \bigoplus_{k=0}^{\lfloor d/2 \rfloor} \mathcal{P}_d^k,$$

as claimed in part (2); taking the direct sum over d yields $\mathcal{P} = \bigoplus_{k=0}^{\infty} \mathbf{F}^k \mathcal{P}^0$, also claimed in part (2). To complete the proof of part (2) we compare the decompositions (2.20) of \mathcal{P}_d and \mathcal{P}_{d-2} and note that $\mathcal{P}_d^k = \mathbf{F}\mathcal{P}_{d-2}^{k-1}$ for each $k > 0$. Part (3) follows because the decomposition (2.20) diagonalizes $\mathbf{F}\Delta|_{\mathcal{P}_d}$. Finally part (4) is again the equality of the $k = 0$ terms in (2.19). \square

Remarks. Part (2) of Proposition 2.5 says in effect that $\mathcal{P} = \bigoplus_{d=0}^{\infty} (\mathcal{P}_d^0 \otimes U_{\frac{n}{2}+d})$, where for any real $m > 0$ we write U_m for the infinite-dimensional irreducible representation of \mathfrak{sl}_2 with basis $\{Y^k v\}_{k=0}^{\infty}$ where $Xv = 0$ and $Hv = -mv$. These U_m come from representations in the “discrete series” of unitary representations of the Lie group $\mathrm{SL}_2(\mathbb{R})$ when n is even (see [Lan75, Chapter IX]); when n is odd, they come from discrete-series representations of the “metaplectic” double cover of $\mathrm{SL}_2(\mathbb{R})$ that do not descend to $\mathrm{SL}_2(\mathbb{R})$.

It also follows from part (2) that $\mathcal{P}_d^0 \cap \mathbf{F}\mathcal{P}_{d-2} = \{0\}$, and thus that \mathcal{P}^0 contains no nonzero multiple of $\langle x, x \rangle$. Proving this was set as problem B-5 on the 2005 Putnam exam, which was the hardest of the 12 problems that year, solved by only five of the top 200 scorers (see [KAL06, p.736 and p. 741]). The solution printed in [KAL06, p. 742] uses some of the ingredients used here to prove Proposition 2.5.

2.5. Weighted Theta Functions. The functional equation (2.6) for theta functions of lattices extends to theta functions weighted by a harmonic polynomial.

Theorem 2.6. *Let L be any lattice in \mathbb{R}^n , and $P : \mathbb{R}^n \rightarrow \mathbb{C}$ any harmonic polynomial of degree d . Then*

$$(2.21) \quad \Theta_{L,P}(e^{-2\pi t}) = i^d \text{Vol}(\mathbb{R}^n/L) t^{-(n/2)-d} \Theta_{L,P}(e^{-2\pi/t})$$

for all $t > 0$.

By the Poisson summation formula, this will follow from the following generalization of (2.7):

Theorem 2.7. *Suppose that $t > 0$ and $P : \mathbb{R}^n \rightarrow \mathbb{C}$ is a harmonic polynomial on \mathbb{R}^n of degree d . Define a function $f : \mathbb{R}^n \rightarrow \mathbb{R}$ by*

$$(2.22) \quad f(x) = P(x) e^{-\pi \langle x, x \rangle t}.$$

Then the Fourier transform of f is

$$(2.23) \quad \hat{f}(y) = i^d t^{-(\frac{n}{2}+d)} P(y) e^{-\pi \langle y, y \rangle / t}.$$

Proof. For $t \in \mathbb{C}$ define an operator

$$(2.24) \quad G_t : C^\infty(\mathbb{R}^n) \rightarrow C^\infty(\mathbb{R}^n), \quad g \mapsto e^{-\pi t \langle x, x \rangle} g$$

that multiplies every C^∞ function by the Gaussian $e^{-\pi t \langle x, x \rangle}$; these operators constitute a one-parameter group: $G_t G_{t'} = G_{t+t'}$ for all t, t' . We are then interested in $f = G_t P$ for $P \in \mathcal{P}$ in the intersection of the kernel of Δ with an eigenspace of E . If $P \in \mathcal{P}_d$ then

$$d \cdot f = G_t(d \cdot P) = G_t E P = (G_t E G_{-t}) G_t P = (G_t E G_{-t}) f,$$

so f is in the d -eigenspace of $G_t E G_{-t}$; likewise $f \in \ker G_t \Delta G_{-t}$. Since our one-parameter group $\{G_t\}$ has infinitesimal generator $-\pi F$, we expect that conjugation by G_t will take Δ, E to some linear combination of Δ, E, F . Indeed we find the following relations.⁶

Lemma 2.8 (Conjugation of Δ, E, F by G_t). *The operators G_t commute with F , and we have*

$$(2.25) \quad G_t E G_{-t} = E + 2\pi t F, \quad G_t \Delta G_{-t} = \Delta + \pi t(4E + 2n) + (2\pi t)^2 F.$$

Proof. As with the commutation relations (2.16), this comes down to an exercise in differential calculus. Here we start from the fact that G_t commutes with each x_j while $G_t(\partial/\partial x_j)G_{-t} = 2\pi t x_j + (\partial/\partial x_j)$, whence the first formula in (2.25) quickly follows, while $G_t F = F G_t$ is immediate. A somewhat longer computation establishes the second formula. \square

Corollary 2.9. *The operators Δ, E, F act on $G_t \mathcal{P}$, and the subspace $G_t \mathcal{P}_d^0$ is the intersection of $\ker(\Delta + \pi t(4E + 2n) + (2\pi t)^2 F)$ with the d -eigenspace of $E + 2\pi t F$ in $G_t \mathcal{P}$.*

We next relate the Fourier transform of a Schwartz function f with the Fourier transforms of its images under Δ, E, F .

Lemma 2.10 (Conjugation of Δ, E, F by the Fourier Transform). *Let $f : \mathbb{R}^n \rightarrow \mathbb{C}$ be any Schwartz function. Then:*

- (1) *For each $j = 1, \dots, n$, the Fourier transform of $x_j f$ is $(2\pi i)^{-1} \partial \hat{f} / \partial y_j$, and the Fourier transform of $\partial f / \partial x_j$ is $-2\pi i y_j \hat{f}$.*
- (2) *The Fourier transforms of Δf , $(2E+n)f$, and Ff are respectively $-(2\pi)^2 F \hat{f}$, $-(2E+n)\hat{f}$, and $-(2\pi)^{-2} \Delta \hat{f}$.*

⁶ This is where it becomes natural to use $\varpi = 2\pi$ when choosing the images of the generators (2.18) of \mathfrak{sl}_2 : conjugation by G_t then takes (X, H, Y) to $(X - tH - t^2 Y, H + 2tY, Y)$; other choices would produce more complicated coefficients.

Proof. Again this is a calculus exercise, here with definite integrals. The formula for the Fourier transform of $\partial f / \partial x_j$ is obtained by integrating by parts with respect to x_j . The Fourier transform of $x_j f$ can be obtained from this using Fourier inversion, or directly by differentiation with respect to y_j of the integral (2.2) that defines $\hat{f}(y)$. We then obtain part (2) by iterating the formulas in part (1) to find the Fourier transform of $\partial^2 f / \partial x_j^2$, $x_j \partial f / \partial x_j$, or $x_j^2 f$, and summing over j . The case of $\mathbf{E}f$ can be explained by writing the operator $2\mathbf{E} + n$ as $\sum_{j=1}^n (x_j (\partial / \partial x_j) + (\partial / \partial x_j) \circ x_j)$. \square

We use this to show that if $f \in \mathbf{G}_t \mathcal{P}$ then $\hat{f} \in \mathbf{G}_{1/t} \mathcal{P}$, that is, that \hat{f} is *some* polynomial multiplied by $e^{-\pi \langle y, y \rangle / t}$. More precisely:

Proposition 2.11. *Let $t \in \mathbb{C}$ with $\operatorname{Re}(t) > 0$. If $f = \mathbf{G}_t P$ for some $P \in \mathcal{P}_d$ then $\hat{f} = \mathbf{G}_{1/t} \hat{P}$ for some $\hat{P} = \sum_{d'=0}^d \hat{P}_{d'}$ with each $\hat{P}_{d'} \in \mathcal{P}_{d'}$ and $\hat{P}_d = i^d t^{-(\frac{n}{2}+d)} P$. As before $t^{-(\frac{n}{2}+d)}$ denotes the $-(n+2d)$ power of the principal square root of t .*

Proof. We use induction on d . The base case $d = 0$ is the fact that the Fourier transform of $e^{-\pi t \langle x, x \rangle}$ is $t^{-n/2} e^{-\pi \langle y, y \rangle / t}$, which we showed already. Suppose we have established the claim for $P \in \mathcal{P}_d$. By linearity and the fact that \mathcal{P}_{d+1} is spanned by its subspaces $x_j \mathcal{P}_d$, it is enough to prove the proposition with P replaced by $x_j P$. By the first part of Lemma 2.10, the Fourier transform of $\mathbf{G}_t x_j P = x_j \mathbf{G}_t P$ is

$$(2.26) \quad \frac{1}{2\pi i} \frac{\partial}{\partial y_j} (\mathbf{G}_{1/t} \hat{P}) = \frac{1}{2\pi i} \mathbf{G}_{1/t} \left(\frac{\partial \hat{P}}{\partial y_j} - \frac{2\pi}{t} y_j \hat{P} \right).$$

By the inductive hypothesis \hat{P} has degree d and leading part $\hat{P}_d = i^d t^{-(\frac{n}{2}+d)} P$. Therefore the right-hand side of (2.26) has degree $d+1$ and leading part

$$\frac{-2\pi t^{-1}}{2\pi i} \hat{P}_d = \frac{i}{t} \hat{P}_d = i^{d+1} t^{-(\frac{n}{2}+d+1)} y_j P.$$

This completes the inductive step and the proof. \square

To finish the proof of Theorem 2.7, suppose $P \in \mathcal{P}_d^0$ and $f(x) = P(x) e^{-\pi \langle x, x \rangle t} = \mathbf{G}_t P$. By Corollary 2.9,

$$(\Delta + \pi t(4\mathbf{E} + 2n) + (2\pi t)^2 \mathbf{F})f = 0, \quad (\mathbf{E} + 2\pi t \mathbf{F})f = d \cdot f.$$

Taking the Fourier transform and applying the second part of Lemma 2.10, we deduce

$$(-(2\pi)^2 \mathbf{F} - \pi t(4\mathbf{E} + 2n) - t^2 \Delta) \hat{f} = 0, \quad -\left(\mathbf{E} + n + \frac{t}{2\pi} \Delta\right) \hat{f} = d \cdot \hat{f}.$$

Eliminating $\Delta \hat{f}$, we find $d \cdot \hat{f} = (\mathbf{E} + \frac{2\pi}{t} \mathbf{F}) \hat{f}$; that is, \hat{f} is in the d -eigenspace of $\mathbf{E} + 2\pi t^{-1} \mathbf{F}$. By Proposition 2.11, we know that $\hat{f} = \mathbf{G}_{1/t} \hat{P}$ for some $\hat{P} \in \mathcal{P}$. By Lemma 2.8, then, \hat{P} is in the d -eigenspace of \mathbf{E} ; that is, $\hat{P} \in \mathcal{P}_d$. By Proposition 2.11, we conclude that $\hat{P} = i^d t^{-(\frac{n}{2}+d)} P$. \square

We have now proven the functional equation (2.21) for weighted theta functions $\Theta_{L,P}$ (Theorem 2.6). This identity is trivial when $d = \deg(P)$ is odd, because then $\Theta_{L,P}$ is identically zero (by cancellation of the v and $-v$ terms), but it gives new information when d is even and positive.

Again we consider the special case of a Type II lattice. Generalizing (2.8), we define

$$(2.27) \quad \theta_{L,P}(\tau) := \Theta_{L,P}(e^{2\pi i \tau}) = \sum_{v \in L} P(v) e^{\pi \langle v, v \rangle i \tau}$$

for $\tau \in \mathcal{H}$. Then $\theta_{L,P}(\tau) = \theta_{L,P}(\tau + 1)$, and Theorem 2.6 gives $\theta_{L,P}(\tau) = t^{-(\frac{n}{2}+d)}\theta_L(-1/\tau)$, with the factor i^d absorbed by the change of variable $\tau = it$ because d is even. It follows as before that

$$(2.28) \quad \theta_{L,P}(\tau) = (c\tau + d)^{-(\frac{n}{2}+d)} \theta_{L,P}\left(\frac{a\tau + b}{c\tau + d}\right)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, so $\theta_{L,P}$ is a modular form of weight $\frac{n}{2} + d$ for $\mathrm{SL}_2(\mathbb{Z})$. Hence $\theta_{L,P}$ is a polynomial in \mathcal{E}_4 and the weight-6 Eisenstein series

$$\mathcal{E}_6 = 1 - 504 \sum_{n=1}^{\infty} \frac{n^5 q^n}{1 - q^n} = 1 - 504q - 16632q^2 - 122976q^3 - \dots$$

Moreover $\theta_{L,P}$ is a cusp form once $d > 0$: the constant coefficient is $P(0)$, which vanishes for nonconstant homogeneous P . Hence once d is positive the polynomial giving $\theta_{L,P}$ in terms of \mathcal{E}_4 and \mathcal{E}_6 is divisible by $\Delta = 12^{-3}(\mathcal{E}_4^3 - \mathcal{E}_6^2)$. (See again [Ser73, Chapter VII].)

In particular $\theta_{L,P} = 0$ when $\frac{n}{2} + d \in \{2, 4, 6, 8, 10, 14\}$ because in those weights the only cusp form is the zero form.⁷ Likewise we have the following observation.

Lemma 2.12. *Suppose $n = 8m$ and $L \subset \mathbb{R}^n$ is an extremal lattice. Then $\theta_{L,P} = 0$ for every nonconstant harmonic polynomial P on \mathbb{R}^n whose degree d satisfies $4(m - 3\lfloor m/3 \rfloor) + d \in \{2, 4, 6, 8, 10, 14\}$. If $L \subset \mathbb{R}^n$ is a Type II lattice of minimal norm $n/12$ then $\theta_{L,P} = 0$ for every harmonic polynomial P on \mathbb{R}^n of degree 2.*

Proof. We saw already that $\theta_{L,P}$ is a cusp form. If L is extremal, the q^k coefficient of $\theta_{L,P}$ vanishes for each $k \leq \lfloor m/3 \rfloor$. Hence $\Delta^{-\lfloor m/3 \rfloor} \theta_{L,P}$ is a cusp form of weight $4(m - 3\lfloor m/3 \rfloor) + d$, and thus vanishes when $4(m - 3\lfloor m/3 \rfloor) + d \in \{2, 4, 6, 8, 10, 14\}$. Likewise if L has minimal norm $n/12$ and P is a quadratic harmonic polynomial then $\Delta^{1-(n/24)} \theta_{L,P}$ is a cusp form of weight 14, so again $\theta_{L,P} = 0$. \square

If L is extremal then Lemma 2.12 applies to 6, 4, or 2 values of d for $n \equiv 0, 8$, or $16 \pmod{24}$ respectively. We exploit these vanishing results in the next section.

2.6. Spherical t -Designs, Extremal Type II Lattices, and the Venkov condition on Niemeier Lattices. For real $\nu > 0$ let $A_\nu : C^\infty(\mathbb{R}^n) \rightarrow \mathbb{C}$ be the functional that takes any function to its average on the sphere $\Sigma_\nu = \{x \in \mathbb{R}^n : \langle x, x \rangle = \nu\}$ with respect to the probability measure on Σ_ν invariant under the orthogonal group. For any positive integer t , a (possibly empty⁸) finite set $D \subset \mathbb{R}^n$ of nonzero vectors of equal norm ν is said to be a (*spherical*) t -design if and only if

$$(2.29) \quad \sum_{v \in D} P(v) = |D| \cdot A_\nu(P)$$

for all $P \in \mathcal{P}$ with $\deg P \leq t$.⁹ By linearity it is enough to check this condition for $P \in \mathcal{P}_d$ for each $d \leq t$, and may assume $d > 0$ because in the case $d = 0$ of a constant polynomial the

⁷ In this setting $\frac{n}{2} + d$ cannot be as small as 2 because $n \geq 8$, but the possibility of weight 2 arises in the proof of Lemma 2.12.

⁸ With this definition \emptyset is a t -design for all t . For most applications only nonempty designs are of interest; for instance it is only when D is nonempty that we can divide both sides of (2.29) by $|D|$ to get the equivalent condition that the average of any polynomial of degree at most t over Σ_ν can be computed by averaging it over $|D|$. But we allow empty designs here, and also later in the coding-theoretic setting, because this simplifies the statements of the results relating lattices with spherical designs.

⁹ See [Del78] for explanation of the term “ r -design” for this property. For $D \neq \emptyset$, the t -design property is one way to make precise the idea that D is “well distributed” in Σ_ν , and better distributed as t grows. One application, and the original one according to [CS99, pp. 89-90], is numerical integration on Σ_ν , using the

condition (2.29) is satisfied automatically. We next prove that it is enough to check (2.29) for *harmonic* polynomials of positive degree. We begin by showing that all such polynomials are in $\ker(A_\nu)$.

Lemma 2.13. *If P is a nonconstant harmonic polynomial then $A_\nu(P) = 0$.*

Proof. Choose any $s > 0$. Since P is homogeneous, $A_\nu(P)$ is a positive multiple of the integral of $G_s P$ over all of \mathbb{R}^n . But this integral is the value of the Fourier transform of $G_s P$ at the origin. By Theorem 2.7 this value is some multiple of $P(0)$. Since $d > 0$ we have $P(0) = 0$, so $A_\nu(P) = 0$ as claimed. \square

Thus our design criterion can be stated as follows.

Lemma 2.14. *A finite subset $D \subset \Sigma_\nu$ is a t -design if and only if $\sum_{v \in D} P(v) = 0$ for all nonconstant harmonic polynomials P of degree at most t .*

Proof. The “only if” direction is immediate from Lemma 2.13. We prove the “if” implication. By the second part of Proposition 2.5 any polynomial of degree $d \leq t$ can be written as $\sum_{k=0}^{\lfloor d/2 \rfloor} F^k P_k$ with each P_k harmonic of degree $d - 2k$. It is thus enough to check (2.29) for each $F^k P_k$. But by hypothesis, (2.29) holds for each P_k (including $P_{d/2}$ if d is even, because then P_k is constant). Since the restriction of each $F^k P_k$ to Σ_ν is $\nu^k P_k$, it follows that (2.29) holds for $F^k P_k$ as well, and we are done. \square

Combining this with Lemma 2.12 yields the following theorem of Venkov [Ven01], which asserts that in an extremal or nearly extremal Type II lattice the vectors of each nonzero norm form a spherical design.

Theorem 2.15. *Let $L \subset \mathbb{R}^n$ be a Type II lattice with minimal norm $2k$. Assume $r := 24k - n$ is nonnegative. Set $t = 3$ if $r = 0$ and $t = (r/2) - 1$ if $r > 0$. Then $L \cap \Sigma_\nu$ is a t -design for every $\nu > 0$.*

Proof. Because $L \cap \Sigma_\nu$ is centrally symmetric, we need only check the criterion of Lemma 2.14 for P of even degree. For such P , Lemma 2.12 applies, so $\theta_{L,P} = 0$. The criterion $A_\nu(P) = 0$ then holds because $A_\nu(P)$ is a coefficient of $\theta_{L,P}$. \square

Remarks. In general $L \cap \Sigma_\nu$ need not be a $(t+1)$ -design: there will be lattice norms ν and harmonic polynomials P of degree $t+1$ whose sum over $L \cap \Sigma_\nu$ is nonzero. However, when $r > 0$ it will be true that the sum over $L \cap \Sigma_\nu$ of any harmonic polynomial of degree $t+3$ vanishes, because there are no nonzero cusp forms of weight 14. Thus each $L \cap \Sigma_\nu$ is what Venkov [Ven01] called a “ $t\frac{1}{2}$ -design”: a finite subset $D \subset \Sigma_\nu$ such that $\sum_{v \in D} P(v) = 0$ for all $P \in \mathcal{P}_d^0$ with either $d \leq t$ or $d = t+3$.

The fact that in each case $L \cap \Sigma_\nu$ is a 2-design already lets us deduce that if $L \cap \Sigma_\nu$ is nonempty then it spans \mathbb{R}^n as a vector space. Indeed if $L \cap \Sigma_\nu$ does not span \mathbb{R}^n then it is contained in a hyperplane $\{x \in \mathbb{R}^n : \langle x, \dot{x} \rangle = 0\}$ for some nonzero $\dot{x} \in \mathbb{R}^n$; then we can take $P(x) = \langle x, \dot{x} \rangle^2$ in (2.29) and observe that each of the terms $P(v)$ in the left-hand side vanishes, while the factor $A_\nu(P)$ of the right-hand side is strictly positive, so the remaining factor $|D|$ must vanish, making $L \cap \Sigma_\nu = \emptyset$ as claimed.

More precise results can often be obtained when ν equals or slightly exceeds the minimal norm, because then any two vectors in $L \cap \Sigma_\nu$ must have integer inner product, and only a few integers can arise, making the condition that $L \cap \Sigma_\nu$ be a t -design or a $t\frac{1}{2}$ -design particularly stringent. We give three examples: configuration results for extremal Type II lattices in several

right-hand side of (2.29) as an approximation to the left-hand side even when P is not polynomial but smooth enough to be well approximated by polynomials.

dimensions, including multiples of 24 up to 96, showing that such lattices are generated by their minimal vectors; Venkov's simplification of Niemeier's classification of Type II lattices in \mathbb{R}^{24} ; and a novel proof of the uniqueness of the E_8 lattice.

Configuration results for extremal Type II lattices. While a nonempty shell $L \cap \Sigma_\nu$ in an external lattice L must generate \mathbb{R}^n as a vector space, it need not generate L over \mathbb{Z} : already $(L, \nu) = (D_{16}^+, 2)$ is a counterexample, since the minimal nonzero vectors of D_{16}^+ generate only the index-2 sublattice D_{16} . Still, for some n it can be proved that every extremal lattice is generated by its vectors of minimal norm $2k$. Let L_0 be the sublattice of L generated by the minimal vectors, and assume $[L : L_0] > 1$. Then there are nonlattice vectors $\dot{v} \in L_0^*$, and $\langle v, \dot{v} \rangle \in \mathbb{Z}$ for all $v \in L \cap \Sigma_{2k}$. If \dot{v} has minimal norm in its coset mod L then $|\langle v, \dot{v} \rangle| \leq k$ for all such v . This together with the t -design or $t\frac{1}{2}$ -design condition on $L \cap \Sigma_{2k}$ yields a contradiction for several values of n , proving that $L_0 = L$ for each of those n . (See [Ven84], [Oze86a], [Oze86b], [Kom09a], and [Elk11].)

Niemeier lattices. Suppose L is a Type II lattice in \mathbb{R}^{24} . Then the hypothesis of Theorem 2.15 is satisfied with $r = 0$ or $r = 24$. In either case we find in particular that $L \cap \Sigma_2$ is a 2-design. But the vectors of norm 2 in any even lattice constitute a root system. Venkov [Ven80], used the condition that this root system be a 2-design to show *a priori* that it must be among the 24 root systems that arise for the Niemeier lattices, and thus to considerably streamline the classification of Type II lattices in \mathbb{R}^{24} .

The uniqueness of E_8 . Finally, let $n = 8$ and let $L \subset \mathbb{R}^8$ be any Type II lattice. Then $\theta_L = \mathcal{E}_4 = 1 + 240q + 2160q^2 + \dots$, and L is automatically extremal, so in particular $L \cap \Sigma_2$ is a 7-design of size 240. We shall use these facts to prove that $L \cong E_8$. There are 2160 vectors of norm 4 in L ; choose one, and call it \dot{x} . Let D be the 7-design $L \cap \Sigma_2$. For $j \in \mathbb{Z}$ let N_j be the number of vectors $x \in D$ such that $\langle x, \dot{x} \rangle = j$. If $N_j \neq 0$, then $|j| \leq \sqrt{8}$ (by Cauchy-Schwarz) and $j \in \mathbb{Z}$ (because $\langle v, v' \rangle \in \mathbb{Z}$ for all $v, v' \in L$); hence $j \in \{-2, -1, 0, 1, 2\}$. Therefore

$$(2.30) \quad \sum_{j=-2}^2 N_j = |D| = 240.$$

Since D is centrally symmetric, $N_{-j} = N_j$ for each j . Finally, since D is a 7-design, (2.29) holds with $P(x) = \langle x, \dot{x} \rangle^d$ for each positive integer $d \leq 7$. This is automatic for d odd, but for $d = 2, 4, 6$ we get linear equations in N_0, N_1, N_2 , and already the $d = 2$ and $d = 4$ equations together with (2.30) let us solve for the N_j . We find

$$(2.31) \quad (N_{-2}, N_{-1}, N_0, N_1, N_2) = (14, 64, 84, 64, 14).$$

(See the Remarks at the end of this section for the evaluation of the functional A_ν on even powers of $\langle x, \dot{x} \rangle$.) In particular there are 14 vectors in D , call them v_i for $1 \leq i \leq 14$, whose inner product with \dot{x} is 2.

For each i we obtain a lattice vector $x_i = 2v_i - \dot{x}$ that is orthogonal to \dot{x} and satisfies $\langle x_i, x_i \rangle = 4$ and $x_i \equiv \dot{x} \pmod{2L}$. For any i and i' we have

$$\begin{aligned} \langle x_i, x_{i'} \rangle &= \langle 2v_i - \dot{x}, 2v_{i'} - \dot{x} \rangle = 4\langle v_i, v_{i'} \rangle - 2\langle v_i, \dot{x} \rangle - 2\langle \dot{x}, v_{i'} \rangle + \langle \dot{x}, \dot{x} \rangle \\ &= 4\langle v_i, v_{i'} \rangle - 4 - 4 + 4 \\ &= 4\langle v_i, v_{i'} \rangle - 4 \\ &\equiv 0 \pmod{4}. \end{aligned}$$

Thus the vectors x_i for $1 \leq i \leq 14$, together with \dot{x} and $-\dot{x}$, are 16 vectors of norm 4, any two of which are equal, opposite, or orthogonal. Hence the x_i together with $\pm\dot{x}$ are the minimal vectors of an isometric copy of $2\mathbb{Z}^8$ in L . Moreover L also contains $v_i = (\dot{x} + x_i)/2$, and

thus contains the \mathbb{Z} -span of \dot{x} and the v_i , which is isometric with D_8 . But L is self-dual, so $D_8^* \subset L \subset D_8$. Of the three lattices satisfying this condition, one is \mathbb{Z}^8 , which is of Type I, and the other two are isomorphic with E_8 . Therefore $L \cong E_8$, as claimed.

Remarks. A related proof, parallel to the beginning of Conway's proof [Con69] of the uniqueness of the Leech lattice, starts from the observation that each of the 2^8 cosets of $2L$ in L intersects $\{v \in L : \langle v, v \rangle \leq 4\}$ in either $\{0\}$, a pair of minimal vectors, or at most 8 orthogonal pairs of vectors of norm 4. This accounts for at least $1 + 240/2 + 2160/16 = 256 = 2^8$ cosets. Hence equality holds throughout, and any of the nonzero cosets that does not meet Σ_2 gives us a copy of D_8 in L . This approach uses only the modularity of θ_L , not of the more general $\theta_{L,P}$, though it applies in fewer cases. Either technique also yields the number of automorphisms of E_8 : there are 2160 choices of \dot{x} , and 2^{77} automorphisms of D_8 that fix \dot{x} , half of which send E_8 to itself, so $|\text{Aut}(E_8)| = 2160 \cdot 2^{67} = 696729600$.

For even $d \geq 0$, and a given vector \dot{x} of norm $\nu > 0$, the average over Σ_ν of $\langle x, \dot{x} \rangle^d$ is computed as a quotient of Beta integrals. We find that if $P(x) = \langle x, \dot{x} \rangle^d$ then

$$(2.32) \quad A_\nu(P) = (\nu\nu)^{d/2} \frac{\int_0^1 u^d (1-u^2)^{(n-3)/2} du}{\int_0^1 (1-u^2)^{(n-3)/2} du} = (\nu\nu)^{d/2} \frac{B((d+1)/2, (n-1)/2)}{B(1/2, (n-1)/2)},$$

where u is the normalized projection $(\nu\nu)^{-1/2} |\langle x, \dot{x} \rangle|$. Thus

$$(2.33) \quad A_\nu(P) = (\nu\nu)^{d/2} \frac{1}{n} \frac{3}{n+2} \frac{5}{n+4} \cdots \frac{d-1}{n+d-2}.$$

In our case $\nu\nu = 2 \cdot 4 = 8$, so $A_\nu(P) = 1, 12/5, 8$ for $d = 2, 4, 6$.

Alternatively we could have applied Lemma 2.14 to the *zonal spherical harmonics*, which are harmonic polynomials that depend only on $\langle x, \dot{x} \rangle$. For each degree d there is a one-dimensional space of zonal spherical harmonics, proportional to a Gegenbauer orthogonal polynomial $C_m^{((n-2)/2)}(u)$ with $u = (\nu\nu)^{-1/2} \langle x, \dot{x} \rangle$. This is equivalent to using (2.32) and (2.33) for t -designs, but for a $t_{\frac{1}{2}}$ -design we need the zonal spherical harmonics to exploit the vanishing of $\sum_{v \in D} P(v)$ for $P \in \mathcal{P}_{t+3}^0$. This, too, has an analogue in the setting of discrete harmonic polynomials, as in the proof of Theorem 9.2 at the end of this paper.

3. WEIGHT ENUMERATORS OF BINARY LINEAR CODES

3.1. Coding-Theoretic Preliminaries. By a (*binary linear*) *code* of length n we mean a vector subspace of the \mathbb{F}_2 -vector space \mathbb{F}_2^n . In this context, vectors of length n over \mathbb{F}_2 are often called (binary) “words” of length n . The (*Hamming*) *weight* of a word $w \in \mathbb{F}_2^n$, denoted by $\text{wt}(w)$, is the number of nonzero coordinates of w , and the (*Hamming*) *distance* between two words $w, w' \in \mathbb{F}_2^n$ is $\text{wt}(w' - w)$. We denote by (\cdot, \cdot) the usual bilinear pairing on \mathbb{F}_2^n , defined by $(v, w) = \sum_{j=1}^n v_j w_j$. For a linear code $C \subseteq \mathbb{F}_2^n$, the *dual code* is the annihilator C^\perp of C with respect to this pairing; thus $\dim(C) + \dim(C^\perp) = n$ and $C^{\perp\perp} = C$ for every linear code $C \subseteq \mathbb{F}_2^n$.

If $C = C^\perp$ then C is *self-dual*. Then $(c, c') = 0$ for all $c, c' \in C$, and in particular $\text{wt}(c)$ is even for all $c \in C$ because $0 = (c, c)$ is the reduction of $\text{wt}(c)$ mod 2. The map $\text{wt} : C \rightarrow \mathbb{Z}$ then reduces mod 4 to a group homomorphism $C \rightarrow 2\mathbb{Z}/4\mathbb{Z}$. The code C is said to be *doubly even* or *of Type II* if this homomorphism is trivial, that is, if $(c, c) \in 4\mathbb{Z}$ for all $c \in C$; otherwise C is said to be *singly even* or *of Type I*. This notation reflects the analogy between binary linear codes and lattices. It also respects the following construction (“Construction A” of [LS71]; see also [CS99, pp. 182–183]) that associates a lattice $L_C \subset \mathbb{R}^n$ to any linear code $C \subseteq \mathbb{F}_2^n$:

$$(3.1) \quad L_C := \{2^{-1/2}v : v \in \mathbb{Z}^n, v \bmod 2 \in C\}.$$

Indeed $L_C^* = L_{C^\perp}$, so L_C is self-dual if and only if C is, in which case L_C is of Type I or Type II according as C is of Type I or Type II, respectively.

Examples. If $C = C^\perp$ then $\dim(C) = n/2$, so n is even. For each positive even integer n there is a Type I code of length n consisting of all c such that $c_{2j-1} = c_{2j}$ for each $j \leq n/2$. This is the unique Type I code for $n = 2$, and is unique up to isomorphism (i.e., up to coordinate permutation) for $n \leq 8$, but not unique for any $n \geq 10$; and as with lattices the number of isomorphism classes grows rapidly with n .

If \mathbb{F}_2^n contains a Type II code then $n \equiv 0 \pmod 8$. (This follows via Construction A from the corresponding theorem for lattices, but can also be proven directly.¹⁰) An example is the *extended Hamming code* in \mathbb{F}_2^8 : if we identify \mathbb{F}_2^8 with the space of \mathbb{F}_2 -valued functions on \mathbb{F}_2^3 , the Hamming code can be constructed as the subspace of affine-linear functions on \mathbb{F}_2^3 . The extended Hamming code is the unique Type II code of length 8; there are two such codes of length 16, nine of length 24, and a rapidly growing number as $n \rightarrow \infty$ through multiples of 8.

3.2. Discrete Poisson Summation. We define the *discrete Fourier transform* (or *Hadamard transform*) \hat{f} of a function $f : \mathbb{F}_2^n \rightarrow \mathbb{C}$ as the function on \mathbb{F}_2^n given by

$$(3.2) \quad \hat{f}(u) = \sum_{v \in \mathbb{F}_2^n} (-1)^{(u,v)} f(v).$$

We review the *discrete Poisson summation formula*, a discrete analog of the Poisson summation formula for lattices (Theorem 2.1). Like its lattice analog, the discrete Poisson summation formula relates the sums of a function to the sums of the function's discrete Fourier transform. Here, however, instead of considering the sums of the function and its Fourier transform over a lattice $L \subset \mathbb{R}^n$ and its dual L^* , we consider the sums of the function and its discrete Fourier transform over a linear code $C \subset \mathbb{F}_2^n$ and over C^\perp , the dual code of C .

Theorem 3.1 (Discrete Poisson Summation Formula). *Let $C \subset \mathbb{F}_2^n$ be a binary linear code of length n , and let f be a function from \mathbb{F}_2^n to \mathbb{C} . Then*

$$(3.3) \quad \sum_{c \in C} f(c) = \frac{1}{|C^\perp|} \sum_{c' \in C^\perp} \hat{f}(c').$$

We briefly recount the standard proof of Theorem 3.1, which is the one presented in [MS83, p. 127].

Proof of Theorem 3.1. By expanding the sum in the right-hand side of (3.3) and rearranging the order of summation, we obtain

$$(3.4) \quad \sum_{c' \in C^\perp} \hat{f}(c') = \sum_{c' \in C^\perp} \sum_{v \in \mathbb{F}_2^n} (-1)^{(c',v)} f(v) = \sum_{v \in \mathbb{F}_2^n} f(v) \sum_{c' \in C^\perp} (-1)^{(c',v)}.$$

¹⁰ Suppose C is a self-dual code of length n . Then C contains the all-1s vector $\mathbf{1}$, because $(v, v) = (v, \mathbf{1})$ for all $v \in \mathbb{F}_2^n$, so $C \subseteq C^\perp$ implies $\mathbf{1} \in C^\perp$. Thus C descends to a vector space of dimension $(n/2) - 1$ in $V := \{0, \mathbf{1}\}^\perp / \{0, \mathbf{1}\}$. Since $2 \mid n$, the perfect pairing (\cdot, \cdot) descends to a perfect pairing on V , so a self-dual code is tantamount to a maximal isotropic subspace of V relative to this pairing. If $4 \mid n$ then the map $\{0, \mathbf{1}\}^\perp \rightarrow \mathbb{F}_2$, $v \mapsto (\text{wt}(v)/2) \pmod 2$ descends to a quadratic form $Q : V \rightarrow \mathbb{F}_2$ consistent with that pairing. A Type II code is then a self-dual code C that is totally isotropic relative to Q . Such C exists if and only if (V, Q) has Arf invariant zero. But the Arf invariant is 0 or 1 according as $\{v \in V : Q(v) = 0\}$ has size $2^{n-3} + 2^{(n/2)-2}$ or $2^{n-3} - 2^{(n/2)-2}$. But this count is $(1/2) \sum_{j=0}^{n/4} \binom{n}{4j} = (1/8) \sum_{\mu^4=1} (1 + \mu)^n = 2^{n-3} + (1/4) \text{Re}(1 + i)^n$, so the result follows from the observation that $(1 + i)^4 = -4$.

Now, whenever $v \in C \subset \mathbb{F}_2^n$ and $c' \in C^\perp$, we have $(c', v) = 0$ by the definition of C^\perp . It follows that the inner sum in (3.4) equals $|C^\perp|$ whenever $v \in C$. Furthermore, when $v \notin C$, the inner sum of (3.4) vanishes.¹¹ The result then follows immediately. \square

3.3. The MacWilliams Identity and Gleason's Theorem. In this section, we recall two classical results from coding theory which are closely related to the theory of lattices. The first of these results, the MacWilliams identity (Theorem 3.2, below), expresses the weight enumerator of C^\perp in terms of the weight enumerator of C . The second result (Theorem 3.3, below) is a famous theorem originally due to Gleason [Gle71], which shows that the weight enumerators of Type II codes can be expressed in terms of two particular weight enumerators.

Theorem 3.2 (MacWilliams Identity ([Mac63]; [CS99, p. 78]; [Ebe02, p. 74]; [MS83, p. 126])). *For any binary linear code C of length n , we have*

$$(3.5) \quad W_C(x, y) = \frac{1}{|C^\perp|} W_{C^\perp}(x + y, x - y).$$

Proof. Define a function $f : \mathbb{F}_2^n \rightarrow \mathbb{C}$ by $f(v) = x^{n-\text{wt}(v)} y^{\text{wt}(v)}$. Then

$$\hat{f}(u) = (x + y)^{n-\text{wt}(u)} (x - y)^{\text{wt}(u)}.$$

Theorem 3.2 therefore follows directly from the discrete Poisson summation formula (Theorem 3.1). \square

Theorem 3.3 (Gleason's Theorem ([Gle71]; [Slo77]; [CS99, p. 192]; [Ebe02, p. 75])). *For any Type II code C , the weight enumerator $W_C(x, y)$ is a polynomial in*

$$(3.6) \quad \varphi_8 := W_{\text{es}}(x, y) = x^8 + 14x^4y^4 + y^8 \quad \text{and} \quad \xi_{24} := x^4y^4(x^4 - y^4)^4.$$

Proof. Since C is of Type II, the exponent of y in each monomial $x^{n-\text{wt}(v)} y^{\text{wt}(v)}$ is a multiple of 4. Thus each monomial is invariant under the substitution of iy for y , whence the sum $W_C(x, y)$ of these monomials also satisfies the identity $W_C(x, y) = W_C(x, iy)$. Since $C = C^\perp$, we also have an identity

$$(3.7) \quad \begin{aligned} W_C(x, y) &= \frac{1}{|C|} W_C(x + y, x - y) \\ &= 2^{-n/2} W_C(x + y, x - y) \\ &= W_C(2^{-1/2}(x + y), 2^{1/2}(x - y)) : \end{aligned}$$

the first step uses Theorem 3.2; for the second, we deduce $|C| = 2^{n/2}$ from $2^n = |C| \cdot |C^\perp| = |C|^2$; and for the last step, we use the fact that W_C is a homogeneous polynomial of degree n . Therefore this homogeneous polynomial is invariant under the group, call it G_Π , generated by linear substitutions with matrices $\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ and $2^{-1/2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

It turns out that G_Π is a complex reflection group, and thus has a polynomial ring of invariants. Namely, G_Π is #9 in the Shephard-Todd list [ST54], and its invariant degrees are 8 and 24, with φ_8, ξ_{24} as a convenient choice of generators. This result completes the proof of Gleason's theorem for Type II codes. \square

In the Appendix we give a direct proof of $\mathbb{C}[x, y]^{G_\Pi} = \mathbb{C}[\varphi_8, \xi_{24}]$. The literature contains several other approaches to the determination of this invariant ring, including Ebeling's proof in [Ebe02] using the theory of modular forms(!). See [CS99, p. 192]. The method we use reaches

¹¹ In this case, (c', v) takes the values 0 and 1 equally often (see [MS83, p. 127]). (This statement is just an instance of the well-known fact that the sum of a nontrivial character on a finite commutative group vanishes.) We could also adapt the technique we used in proving Theorem 2.1, obtaining discrete Poisson summation via the discrete Fourier expansion of the function $z \mapsto \sum_{c \in C} f(c + z)$.

G_{II} via a suitable tower of reflection groups starting from $\{1\}$, each normal in the next; along the way we also obtain Gleason's theorem for Type I codes, and encounter a polynomial ψ_{12} , invariant under an index-2 subgroup of G_{II} , that will figure in our subsequent development.

4. THE SPACES OF DISCRETE HARMONIC POLYNOMIALS

In this section, we present some useful results in the theory of *discrete harmonic polynomials*. These polynomials were originally introduced by Delsarte [Del78], who gave a combinatorial development. Here, we give a new approach to these polynomials using the finite-dimensional representation theory of \mathfrak{sl}_2 .

4.1. Basic Definitions and Notation. A function g on \mathbb{F}_2 may be interpreted as a 2×1 matrix $g = \begin{pmatrix} g_0 \\ g_1 \end{pmatrix}$, where g_v is the value assumed on input $v \in \mathbb{F}_2$. It is easily computed that the discrete Fourier transform \hat{g} of g is the function

$$\hat{g} = \begin{pmatrix} g_0 + g_1 \\ g_0 - g_1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} g_0 \\ g_1 \end{pmatrix};$$

the discrete Fourier transform is therefore encoded by the matrix $\mathsf{T} := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. There is a natural action of \mathfrak{sl}_2 on these functions g , defined by multiplication from the left by matrices in \mathfrak{sl}_2 . Thus, we may interpret the space of functions on \mathbb{F}_2 as a representation of \mathfrak{sl}_2 isomorphic with the 2-dimensional defining representation V_1 of \mathfrak{sl}_2 .

More generally, a monomial function g on \mathbb{F}_2^n must have total degree at most n ,¹² and so may be interpreted as a pure tensor in $V_1^{\otimes n}$; such a function is denoted

$$g = \begin{pmatrix} g_{10} \\ g_{11} \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} g_{n0} \\ g_{n1} \end{pmatrix}$$

and assumes the value $g_{1v_1} \cdots g_{nv_n}$ on $v \in \mathbb{F}_2^n$. In this setting, the discrete Fourier transform corresponds to the action of the operator

$$(4.1) \quad \tilde{\mathsf{T}} := \mathsf{T}^{\otimes n}.$$

For example, the degree- n monomial $g_*(v) = v_1 \cdots v_n$, which takes the value of the product of the coordinates of the input $v \in \mathbb{F}_2^n$, is the function

$$g_* = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

The discrete Fourier transform \hat{g}_* of g_* is

$$\hat{g}_* = \tilde{\mathsf{T}} g_* = \begin{pmatrix} 1 \\ -1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 \\ -1 \end{pmatrix}.^{13}$$

4.1.1. Polynomials in the Variables $(-1)^{v_j}$ ($1 \leq j \leq n$). Instead of working with polynomials in the variables v_j ($1 \leq j \leq n$), we work with the discrete Fourier transforms $(-1)^{v_j}$ ($1 \leq j \leq n$) of these variables.¹⁴ We denote by \mathscr{D} the \mathbb{C} -vector space of polynomial functions Q in the variables

$$(-1)^{v_1}, \dots, (-1)^{v_n},$$

where $v \in \mathbb{F}_2^n$. We denote by \mathscr{D}_d the subspace of \mathscr{D} consisting of degree- d homogeneous polynomials in the $(-1)^{v_j}$ ($1 \leq j \leq n$) with each variable $(-1)^{v_j}$ in each term appearing to degree 0 or 1. We adopt the convention that $\mathscr{D}_d = \{0\}$ for $d < 0$.

¹²This is a consequence of the fact that, for any $v \in \mathbb{F}_2^n$, we have $v_j^2 = v_j$ for all j ($1 \leq j \leq n$).

¹³Note that this aligns with the expression

$$\hat{g}_*(u) = \sum_{v \in \mathbb{F}_2^n} (-1)^{(u,v)} g_*(v) = (-1)^{\sum_{j=1}^n u_j},$$

obtained from the more common definition (3.2) of the discrete Fourier transform given earlier.

¹⁴Delsarte [Del78] uses the v_j basis, rather than the $(-1)^{v_j}$ basis. We depart from Delsarte's notation because the use of the $(-1)^{v_j}$ basis greatly simplifies our development.

The preceding discussion shows that any $Q \in \mathcal{D}$ may be interpreted as an element of $V_1^{\otimes n}$, and that the discrete Fourier transform \tilde{Q} of Q is equal to $\tilde{T}Q$. The action of \mathfrak{sl}_2 defined above gives rise to the following action on \mathcal{D} : if $M \in \mathfrak{sl}_2$ and $Q \in \mathcal{D}$, then the action of M on Q is given by

$$\left(\sum \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots \otimes M \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) Q.$$

Here, $\sum \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots \otimes M \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ denotes the operator equal to

$$(M \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}) + \cdots + (\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots \otimes M \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}) + \cdots + (\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots \otimes M),$$

the sum of n tensors, the j -th of which acts as M on the j -th factor and as the identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ on the other factors.

4.1.2. Conjugation of X , H , and Y by the Discrete Fourier Transform. Recall that we denote by (X, H, Y) the standard basis for \mathfrak{sl}_2 , exhibited in (2.18). We define the operators X' , H' , and Y' to be the conjugates of X , H , and Y by the discrete Fourier transform:

$$\begin{aligned} (4.2) \quad X' &:= T^{-1}XT = \frac{1}{2}(H - X + Y), \\ H' &:= T^{-1}HT = X + Y, \\ Y' &:= T^{-1}YT = \frac{1}{2}(H + X - Y). \end{aligned}$$

Conjugation by the Fourier transform operator T induces an isomorphism of Lie algebras

$$(4.3) \quad X \longleftrightarrow X', \quad H \longleftrightarrow H', \quad Y \longleftrightarrow Y',$$

hence these operators X', H', Y' satisfy the commutation relations of (2.17):

$$(4.4) \quad [X', Y'] = H', \quad [H', X'] = 2X', \quad [H', Y'] = -2Y'.$$

We write \tilde{X}' , \tilde{H}' , and \tilde{Y}' for operators

$$\begin{aligned} (4.5) \quad \tilde{X}' &:= \sum \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots \otimes X' \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \tilde{T}^{-1} \left(\sum \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots \otimes X \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) \tilde{T}, \\ \tilde{H}' &:= \sum \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots \otimes H' \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \tilde{T}^{-1} \left(\sum \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots \otimes H \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) \tilde{T}, \\ \tilde{Y}' &:= \sum \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots \otimes Y' \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \tilde{T}^{-1} \left(\sum \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots \otimes Y \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) \tilde{T}, \end{aligned}$$

which represent the actions of X' , H' and Y' on elements of $V_1^{\otimes n}$. The commutation relations of (4.4) extend to these operators, as well:

$$(4.6) \quad [\tilde{X}', \tilde{Y}'] = \tilde{H}', \quad [\tilde{H}', \tilde{X}'] = 2\tilde{X}', \quad [\tilde{H}', \tilde{Y}'] = -2\tilde{Y}'.$$

The relations (4.6) induce an isomorphism between \mathfrak{sl}_2 and the algebra generated by \tilde{X}' , \tilde{H}' , and \tilde{Y}' .

Now, we have the following result immediately from the definition of \tilde{H}' .

Lemma 4.1. *If $Q \in \mathcal{D}_d$, then $\tilde{H}'Q = (n - 2d)Q$.*

Proof. The result follows directly, because the 1-eigenspace of H' is the span of $\left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$ and the (-1) -eigenspace of H' is the span of $\left\{ \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$. \square

For $Q \in \mathcal{D}_d$, we observe that $(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots \otimes X' \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix})Q \in \mathcal{D}_{d-1}$, as we have

$$X' \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \text{and} \quad X' \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Thus, $\tilde{X}'Q = (\sum (\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}) \otimes \cdots \otimes X' \otimes \cdots \otimes (\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}))Q \in \mathcal{D}_{d-1}$. We define the *space of degree- d discrete harmonic polynomials* by

$$(4.7) \quad \mathcal{D}_d^0 := \ker \left(\tilde{X}' : \mathcal{D}_d \rightarrow \mathcal{D}_{d-1} \right).$$

We then define the *space of discrete harmonic polynomials*, denoted \mathcal{D}^0 , to be the direct sum

$$(4.8) \quad \mathcal{D}^0 := \bigoplus_{d=0}^n \mathcal{D}_d^0 = \ker \left(\tilde{X}' : \mathcal{D} \rightarrow \mathcal{D} \right).$$

4.2. Decomposition of Degree- d Discrete Homogeneous Polynomials. It is immediate from (4.6) that the operator \tilde{H}' maps \mathcal{D}^0 to itself, since if $Q \in \mathcal{D}^0$ then

$$\tilde{X}'\tilde{H}'Q = \left(\tilde{H}'\tilde{X}' - [\tilde{H}', \tilde{X}'] \right) Q = \left(\tilde{H}'\tilde{X}' - 2\tilde{X}' \right) Q = 0.$$

The next lemma substantially refines this observation. Recall [Ser87, p.18, Definition 1] that an element e of an \mathfrak{sl}_2 module is said to be *primitive of weight λ* if $e \neq 0$, $Xe = 0$, and $He = \lambda e$.

Lemma 4.2. *If $Q \in \mathcal{D}_d^0$, then Q is either zero or primitive of weight $n - 2d$ with respect to the representation of \mathfrak{sl}_2 induced by the action of \tilde{X}' , \tilde{H}' , and \tilde{Y}' .*

Proof. The result is a direct consequence of Lemma 4.1 because all $Q \in \mathcal{D}^0$ satisfy $\tilde{X}'Q = 0$. \square

Corollary 4.3. *If $d > n/2$ then $\mathcal{D}_d^0 = \{0\}$.*

Proof. Since \mathcal{D} is finite-dimensional, a primitive vector must have nonnegative weight. \square

For $d \leq n/2$ and $k = 0, 1, \dots, d$, we define $\mathcal{D}_d^k := (\tilde{Y}')^k \mathcal{D}_{d-k}^0$.¹⁵ Combining Lemma 4.2 with the representation theory of \mathfrak{sl}_2 , we now obtain a decomposition result for \mathcal{D}_d similar to that obtained for \mathcal{P}_d in Proposition 2.5.

Proposition 4.4. *For any $d \leq n/2$, we have the following results.*

- (1) *The map $\tilde{X}' : \mathcal{D}_d \rightarrow \mathcal{D}_{d-1}$ is surjective.*
- (2) *We have the direct sum decomposition $\mathcal{D}_d = \bigoplus_{k=0}^d \mathcal{D}_d^k = \mathcal{D}_d^0 \oplus \tilde{Y}'\mathcal{D}_{d-1}$.*
- (3) *For any nonzero $Q \in \mathcal{D}_d$, the space spanned by $\{(\tilde{Y}')^j Q\}_{j=0}^{n-2d}$ is an irreducible \mathfrak{sl}_2 -module isomorphic to $V_{n-2d} := \text{Sym}^{n-2d}(V_1)$.*
- (4) $\dim(\mathcal{D}_d^0) = \dim(\mathcal{D}_d) - \dim(\mathcal{D}_{d-1}) = \binom{n}{d} - \binom{n}{d-1}$.

Proof. This follows quickly from Lemma 4.2 together with the finite-dimensional representation theory of \mathfrak{sl}_2 ; see for instance [Ser87, Chapter IV]. The first and second parts follow from the decomposition of any finite-dimensional \mathfrak{sl}_2 -module as a direct sum of irreducible modules, together with the explicit action of \mathfrak{sl}_2 on each of its finite-dimensional irreducible modules [Ser87, Chapter IV, Theorems 2 and 3]. The third part follows from the structure of the irreducible representation generated by a primitive element of given weight [Ser87, Chapter IV, Corollary 2 of Theorem 1]. The fourth part follows from the first part. \square

It also follows that $\tilde{X}' : \mathcal{D}_d \rightarrow \mathcal{D}_{d-1}$ is injective if $d - 1 \geq n/2$, and thus an isomorphism if $n = 2d - 1$; more generally, if $d \geq n/2$ then $\tilde{X}'^{2d-n} : \mathcal{D}_d \rightarrow \mathcal{D}_{n-d}$ is an isomorphism.

¹⁵The notation \mathcal{D}_d^k is consistent with the notation \mathcal{D}_d^0 for the space of degree- d discrete harmonic polynomials.

5. THE GENERALIZED MACWILLIAMS IDENTITY FOR HARMONIC WEIGHT ENUMERATORS

For a length- n binary linear code $C \subset \mathbb{F}_2^n$ and a discrete harmonic polynomial Q , the harmonic weight enumerator $W_{C,Q}(x, y)$ is defined by

$$(5.1) \quad W_{C,Q}(x, y) := \sum_{c \in C} Q(c) x^{n-\text{wt}(c)} y^{\text{wt}(c)}.$$

This function encodes the weights and distribution of the codewords of C , as the weighted theta functions of a lattice L encode the norms and distribution of the vectors of L .

We now derive a generalized MacWilliams identity for harmonic weight enumerators.

Theorem 5.1. *For any binary linear code $C \subset \mathbb{F}_2^n$ and $Q \in \mathcal{D}_d^0$, the harmonic weight enumerator $W_{C,Q}(x, y) = \sum_{c \in C} Q(c) x^{n-\text{wt}(c)} y^{\text{wt}(c)}$ satisfies the identity*

$$(5.2) \quad W_{C,Q}(x, y) = \left(-\frac{xy}{x^2 - y^2} \right)^d \cdot \frac{2^{\frac{n}{2}+d}}{|C^\perp|} \cdot W_{C^\perp, Q} \left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}} \right).$$

Theorem 5.1 was first proven by Bachoc [Bac99], via a purely combinatorial argument. Here, we give a new proof of this result in analogy with the proof of Theorem 2.6.

5.1. Derivation of the Identity. For $Q \in \mathcal{D}$, the function $Q(v) x^{n-\text{wt}(v)} y^{\text{wt}(v)}$ corresponds in the tensor representation to the function

$$\left(\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}^{\otimes n} \right) Q.$$

Therefore, in analogy with the Gaussian operators G_t defined in Section 2.5, we introduce the operators

$$(5.3) \quad W := \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}, \quad \tilde{W} := W^{\otimes n},$$

$$(5.4) \quad V := \begin{pmatrix} x+y & 0 \\ 0 & x-y \end{pmatrix}, \quad \tilde{V} := V^{\otimes n}.$$

The operator \tilde{W} serves as a sort of “discrete Gaussian” for weight enumerators. Indeed, the weight enumerator $W_C(x, y)$ of a length- n binary linear code is given by

$$(5.5) \quad W_C(x, y) = \sum_{c \in C} \left(\tilde{W} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}^{\otimes n} \right) (c),$$

and the Fourier transform of $\tilde{W} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}^{\otimes n}$ is equal to $\tilde{V} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}^{\otimes n}$.

Lemma 5.2. *If $Q \in \mathcal{D}_d$, then we have*

$$(\tilde{V}^{-1} \tilde{T} \tilde{W}) Q = \hat{Q},$$

where $\hat{Q} = \sum_{d'=0}^d \hat{Q}_{d'}$ with $\hat{Q}_{d'} \in \mathcal{D}_d$ for each d' ($0 \leq d' \leq d$) and

$$(5.6) \quad \hat{Q}_d = \left(-\frac{2xy}{x^2 - y^2} \right)^d Q.$$

Proof. We proceed by strong induction on d . The base case $d = 0$ is immediate, so we suppose that the result holds for $Q \in \mathcal{D}_{d_1}$ for each nonnegative $d_1 \leq d$, and deduce that the result holds also for $Q \in \mathcal{D}_{d+1}$.

The discrete Fourier transform operator is linear, hence it suffices to prove the result for the polynomials of the form $(-1)^{v_j} \cdot Q$ with $Q \in \mathcal{D}_d$. Now, we compute the value of $\tilde{V}^{-1} \tilde{T}$ times

$$(-1)^{v_j} \cdot Q(v) \cdot x^{n-\text{wt}(v)} y^{\text{wt}(v)} = \tilde{W} \cdot \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) \cdot Q$$

explicitly. We find that

$$\begin{aligned}
 & \tilde{V}^{-1} \tilde{T} \left(\tilde{W} \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) Q \right) \\
 &= (\tilde{V}^{-1} \tilde{T} \tilde{W}) \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) (\tilde{V}^{-1} \tilde{T} \tilde{W})^{-1} (\tilde{V}^{-1} \tilde{T} \tilde{W}) Q \\
 &= \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 0 & \frac{x-y}{x+y} \\ \frac{x+y}{x-y} & 0 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) (\tilde{V}^{-1} \tilde{T} \tilde{W}) Q \\
 (5.7) \quad &= \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 0 & \frac{x-y}{x+y} \\ \frac{x+y}{x-y} & 0 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) \hat{Q},
 \end{aligned}$$

where the last equality in (5.7) follows on applying the inductive hypothesis to $(\tilde{V}^{-1} \tilde{T} \tilde{W}) Q$.

It is clear that the right-hand side of (5.7) has maximal degree $d+1$, since \hat{Q} is of degree d and

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 0 & \frac{x-y}{x+y} \\ \frac{x+y}{x-y} & 0 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

is the identity on all but one coordinate. To finish the proof of the lemma, we compute the degree- $(d+1)$ term of (5.7). Now, since

$$\begin{pmatrix} 0 & \frac{x-y}{x+y} \\ \frac{x+y}{x-y} & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{x^2 + y^2}{x^2 - y^2} \begin{pmatrix} 1 \\ 1 \end{pmatrix} - \frac{2xy}{x^2 - y^2} \begin{pmatrix} 1 \\ -1 \end{pmatrix},$$

the degree- $(d+1)$ term of (5.7) must equal $-\frac{2xy}{x^2 - y^2} \hat{Q}_d$.¹⁶ The desired expression (5.6) then follows from the inductive hypothesis. \square

Lemma 5.3. *If $Q \in \mathcal{D}^0$ and $\tilde{H}'Q = \lambda \cdot Q$, then*

- (1) $(\tilde{V}^{-1} \tilde{T} \tilde{W}) \tilde{X}' (\tilde{V}^{-1} \tilde{T} \tilde{W})^{-1} Q = 0$ and
- (2) $(\tilde{V}^{-1} \tilde{T} \tilde{W}) \tilde{H}' (\tilde{V}^{-1} \tilde{T} \tilde{W})^{-1} Q = \lambda \cdot Q$.

Proof. Explicit computation gives

$$(5.8) \quad (\tilde{V}^{-1} \tilde{T} \tilde{W}) \tilde{X}' (\tilde{V}^{-1} \tilde{T} \tilde{W})^{-1} = -\frac{x^2 - y^2}{2xy} \cdot \tilde{X}',$$

$$(5.9) \quad (\tilde{V}^{-1} \tilde{T} \tilde{W}) \tilde{H}' (\tilde{V}^{-1} \tilde{T} \tilde{W})^{-1} = \tilde{H}' + \frac{x^2 + y^2}{xy} \cdot \tilde{X}'.$$

The first and second results follow directly from (5.8) and (5.9), respectively, since

$$Q \in \mathcal{D}^0 = \ker(\tilde{X}'). \quad \square$$

Corollary 5.4. *The operators \tilde{X}' and \tilde{H}' act on $(\tilde{V}^{-1} \tilde{T} \tilde{W}) \mathcal{D}^0$. The subspace $(\tilde{V}^{-1} \tilde{T} \tilde{W}) \mathcal{D}_d^0$ is the intersection of $\ker(\tilde{X}')$ and the $(n-2d)$ -eigenspace of $\tilde{H}' + \frac{x^2 + y^2}{xy} \tilde{X}'$ in $(\tilde{V}^{-1} \tilde{T} \tilde{W}) \mathcal{D}_d^0$.*

5.1.1. Proof of the Generalized MacWilliams Identity. As a final step en route to Theorem 5.1, we prove an expression analogous to Proposition 2.11 for the discrete Fourier transform of the product of \tilde{W} and a discrete harmonic polynomial $Q \in \mathcal{D}_d^0$.

Proposition 5.5. *If $Q \in \mathcal{D}_d^0$, then*

$$(5.10) \quad (\tilde{V}^{-1} \tilde{T} \tilde{W}) Q = \left(-\frac{2xy}{x^2 - y^2} \right)^d Q.$$

¹⁶ Here, \hat{Q}_d is the degree- d term of \hat{Q} , as in the lemma statement.

Proof. From Corollary 5.4, we see that $(\tilde{V}^{-1}\tilde{T}\tilde{W})Q$ is in both \mathcal{D}^0 and (since then $\tilde{H}'Q = 0$) the $(n - 2d)$ -eigenspace of \tilde{H}' . That is, $(\tilde{V}^{-1}\tilde{T}\tilde{W})Q \in \mathcal{D}_d^0$. The result then follows immediately from Lemma 5.2. \square

Finally, we obtain the generalized MacWilliams identity by combining Proposition 5.5 with the discrete Poisson summation formula (Theorem 3.1).

Proof of Theorem 5.1. We obtain the discrete Fourier transform of $\tilde{W}Q$ from Proposition 5.5:

$$(5.11) \quad \tilde{T}(\tilde{W}Q) = \left(\frac{-2xy}{x^2 - y^2}\right)^d \tilde{V}Q = \left(\frac{-2xy}{x^2 - y^2}\right)^d \cdot 2^{n/2} \cdot \left(\begin{pmatrix} \frac{x+y}{\sqrt{2}} & 0 \\ 0 & \frac{x-y}{\sqrt{2}} \end{pmatrix}^{\otimes n}\right) \cdot Q.$$

The desired formula (5.2) then follows directly from (5.11), upon applying Theorem 3.1. \square

Remark. One interesting consequence of Theorem 5.1 is the fact that $W_{C,Q}(x, y)/(xy)^d$ is a polynomial, for any $Q \in \mathcal{D}_d^0$.

Corollary 5.6. *For C a binary linear code and $Q \in \mathcal{D}_d^0$,*

$$\frac{W_{C,Q}(x, y)}{(xy)^d}$$

is a polynomial in the variables x, y .

Proof. By Theorem 5.1,

$$(5.12) \quad \frac{W_{C,Q}(x, y)}{(xy)^d} = \left(-\frac{1}{x^2 - y^2}\right)^d \cdot \frac{2^{\frac{n}{2}+d}}{|C^\perp|} \cdot W_{C^\perp, Q}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right).$$

The left-hand side is a rational function in x, y whose denominator divides $(xy)^d$, and the right-hand side is a rational function whose denominator divides $(x^2 - y^2)^d$. Since $(xy)^d$ and $(x^2 - y^2)^d$ are relatively prime, (5.12) is an identity between polynomials in x and y . \square

As we see at the end of Section 7, Corollary 5.6 also follows directly from the \mathfrak{sl}_2 development of discrete harmonic polynomials.

5.2. A Generalization of Gleason's Theorem. In addition to the generalized MacWilliams identity, Bachoc [Bac99] obtained a harmonic weight enumerator generalization of Gleason's theorem. As we will use this result in Section 7, we state it here.

Theorem 5.7 (Bachoc [Bac99]). *Let C be a Type II code of length n and let $Q \in \mathcal{D}_d^0$. Then, the harmonic weight enumerator $W_{C,Q}(x, y)$ is an element of the principal module $\mathbb{C}[\varphi_8, \xi_{24}]\psi_d$ for the polynomial algebra $\mathbb{C}[\varphi_8, \xi_{24}]$, whose generator is given by*

$$(5.13) \quad \psi_d := \begin{cases} 1 & d \equiv 0 \pmod{4}, \\ x^3 y^3 (x^4 - y^4)^2 (x^8 - y^8) (x^8 - 34x^4 y^4 + y^8) & d \equiv 1 \pmod{4}, \\ x^2 y^2 (x^4 - y^4)^2 & d \equiv 2 \pmod{4}, \\ xy(x^8 - y^8)(x^8 - 34x^4 y^4 + y^8) & d \equiv 3 \pmod{4}. \end{cases}$$

The degree-12 polynomial ψ_2 is a square root of ξ_{24} ; thus the harmonic enumerators that can arise for even d are elements of the polynomial ring $\mathbb{C}[\varphi_8, \psi_2]$, which is the ring of invariants for a complex reflection group contained with index 2 in G_{II} (see the Appendix). For odd d , the polynomials ψ_d are more complicated covariants of G_{II} ; we have $\psi_1 = \psi_2 \psi_3$ and $\psi_3^2 = \psi_2(\varphi_8^3 - 108\xi_{24})$.

6. ZONAL HARMONIC POLYNOMIALS

We now introduce the *zonal harmonic polynomials*, a class \mathcal{ZD}^0 of discrete harmonic polynomials analogous to the zonal spherical harmonics mentioned at the end of Section 2. Specifically, we fix some $\dot{v} \in \mathbb{F}_2^n$ and some d with $0 \leq d \leq \text{wt}(\dot{v})$, and determine the space $\mathcal{ZD}_d^0 \subset \mathcal{D}_d^0$ of degree- d discrete harmonic polynomials invariant under coordinate permutations fixing \dot{v} .

6.1. Preliminaries. Throughout, we fix $\dot{v} \in \mathbb{F}_2^n$. We denote by $\mathcal{ZD}_d \subset \mathcal{D}_d$ the space of degree- d discrete homogeneous polynomials invariant under the group of coordinate permutations fixing \dot{v} , and set $\mathcal{ZD}_d^0 := \mathcal{ZD}_d \cap \mathcal{D}_d^0$. We say that a polynomial in \mathcal{ZD}_d^0 is a *zonal harmonic polynomial of degree d* , and we define the space \mathcal{ZD}^0 of *zonal harmonic polynomials* by

$$(6.1) \quad \mathcal{ZD}^0 := \bigoplus_{d=0}^{\text{wt}(\dot{v})} \mathcal{ZD}_d^0.$$

6.1.1. Generators of \mathcal{ZD}_d . We now fix some d with $0 \leq d \leq \text{wt}(\dot{v})$ and let

$$C_{1;\dot{v}} := \{j : \dot{v}_j = 1\}, \quad C_{0;\dot{v}} := \{j : \dot{v}_j = 0\}.$$

Now, we denote by $Q_{d,k;\dot{v}}(v)$ the degree- d discrete polynomial

$$(6.2) \quad \begin{aligned} Q_{d,k;\dot{v}}(v) &:= \sum_{\substack{\{j_1, \dots, j_k\} \subseteq C_{1;\dot{v}} \\ \{j_{k+1}, \dots, j_d\} \subseteq C_{0;\dot{v}}}} (-1)^{(v_{j_1} + \dots + v_{j_k}) + (v_{j_{k+1}} + \dots + v_{j_d})} \\ &= \sum_{\substack{\{j_1, \dots, j_k\} \subseteq C_{1;\dot{v}} \\ \{j_{k+1}, \dots, j_d\} \subseteq C_{0;\dot{v}}}} (-1)^{v_{j_1}} \dots (-1)^{v_{j_k}} \cdot (-1)^{v_{j_{k+1}}} \dots (-1)^{v_{j_d}} \in \mathcal{D}_d. \end{aligned}$$

The sum is nonempty for all d ($0 \leq d \leq \text{wt}(\dot{v})$) since $|C_{1;\dot{v}}| = \text{wt}(\dot{v})$ and $|C_{0;\dot{v}}| = n - \text{wt}(\dot{v})$.

By construction, it is clear that $Q_{d,k;\dot{v}} \in \mathcal{ZD}_d$. Conversely, we have the following lemma.

Lemma 6.1. *The polynomials $\{Q_{d,k;\dot{v}}\}_{k=0}^{\text{wt}(\dot{v})}$ generate \mathcal{ZD}_d .*

Proof. The result follows immediately from the requirement that any $Q \in \mathcal{ZD}_d$ be invariant under all permutations simultaneously permuting the $\text{wt}(\dot{v})$ nonzero coordinates of \dot{v} and the $n - \text{wt}(\dot{v})$ vanishing coordinates in \dot{v} , together with the fact that the multilinear monomials in the variables $(-1)^{v_j}$ are a basis for \mathcal{D} . \square

Additionally, we have a combinatorial formula for $Q_{d,k;\dot{v}}(v)$.

Proposition 6.2. *We have*

$$(6.3) \quad Q_{d,k;\dot{v}}(v) = \left(\sum_{i=0}^k (-1)^i \binom{\text{wt}(v \cap \dot{v})}{i} \binom{\text{wt}(\dot{v}) - \text{wt}(v \cap \dot{v})}{k-i} \right) \times \left(\sum_{i=0}^{d-k} \binom{\text{wt}(v) - \text{wt}(v \cap \dot{v})}{i} \binom{(n - \text{wt}(\dot{v})) - (\text{wt}(v) - \text{wt}(v \cap \dot{v}))}{d-k-i} \right).$$

The proof of Proposition 6.2 is immediately obtained from evaluation of the expression (6.2) for $Q_{d,k;\dot{v}}$.

6.1.2. *The action of \tilde{X}' on $Q_{d,k;\dot{v}}$.* Now, we determine the action of \tilde{X}' on the polynomials $\{Q_{d,k;\dot{v}}\}_{k=0}^{\text{wt}(\dot{v})}$.

Lemma 6.3. *We have*

$$(6.4) \quad \tilde{X}'Q_{d,k;\dot{v}} = ((n - \text{wt}(\dot{v})) - (d - k - 1))Q_{d-1,k;\dot{v}} + (\text{wt}(\dot{v}) - (k - 1))Q_{d-1,k-1;\dot{v}}.$$

Proof. First, we observe that

$$(6.5) \quad \tilde{X}' \cdot ((-1)^{v_{j_0} + \dots + v_{j_d}}) = \sum_{\ell=1}^d (-1)^{v_{j_0} + v_{j_1} + \dots + v_{j_{\ell-1}} + v_{j_{\ell+1}} + \dots + v_{j_d} + v_{j_{d+1}}},$$

where we have used the convention that $v_{j_0} = 0 = v_{j_{d+1}}$.¹⁷ It then follows from (6.5) that

$$\tilde{X}'Q_{d,k;\dot{v}} = b_k \cdot Q_{d-1,k;\dot{v}} + b_{k-1} \cdot Q_{d-1,k-1;\dot{v}}$$

for constants $b_k, b_{k-1} \in \mathbb{Z}$. To see that

$$b_{k-1} = \text{wt}(\dot{v}) - (k - 1),$$

we observe that each monomial term in $Q_{d-1,k;\dot{v}}$ can arise from $\text{wt}(\dot{v}) - (k - 1)$ different monomial terms in $Q_{d,k;\dot{v}}$. Likewise, we obtain

$$b_k = (n - \text{wt}(\dot{v})) - (d - k - 1). \quad \square$$

6.2. Determination of the Zonal Harmonic Polynomials. We now combine Lemma 6.1 and Lemma 6.3 to characterize \mathcal{ZD}_d^0 .

Proposition 6.4. *If $Q \in \mathcal{ZD}_d^0$, then $Q = b_0 \cdot Q_{d;\dot{v}}$ for some constant $b_0 \in \mathbb{C}$, where*

$$(6.6) \quad Q_{d;\dot{v}}(v) := \sum_{k=0}^d (-1)^k \left(\prod_{\ell=0}^{k-1} \frac{(n - \text{wt}(\dot{v})) - (d - \ell - 1)}{\text{wt}(\dot{v}) - \ell} \right) Q_{d,k;\dot{v}}(v).$$

Proof. We consider some $Q \in \mathcal{ZD}_d^0 = \mathcal{ZD}_d \cap \mathcal{D}_d^0$. By Lemma 6.1, there exist constants $\{b_k\}_{k=0}^{\text{wt}(\dot{v})} \subset \mathbb{C}$ such that

$$Q = \sum_{k=0}^{\text{wt}(\dot{v})} b_k \cdot Q_{d,k;\dot{v}}.$$

Since $Q \in \mathcal{D}_d^0$, we have

$$\begin{aligned} 0 &= \tilde{X}'Q = \tilde{X}' \left(\sum_{k=0}^{\text{wt}(\dot{v})} b_k \cdot Q_{d,k;\dot{v}} \right) = \sum_{k=0}^{\text{wt}(\dot{v})} b_k \cdot \tilde{X}'Q_{d,k;\dot{v}} \\ &= \sum_{k=0}^{\text{wt}(\dot{v})} b_k \cdot (((n - \text{wt}(\dot{v})) - (d - k - 1))Q_{d-1,k;\dot{v}} + (\text{wt}(\dot{v}) - (k - 1))Q_{d-1,k-1;\dot{v}}) \\ &= \sum_{k=0}^{\text{wt}(\dot{v})} \left(b_k((n - \text{wt}(\dot{v})) - (d - k - 1)) + b_{k+1}(\text{wt}(\dot{v}) - (k)) \right) Q_{d-1,k;\dot{v}}. \end{aligned}$$

(The penultimate equality follows from Lemma 6.3.) By comparing coefficients, we then obtain

$$b_{k+1} = -\frac{(n - \text{wt}(\dot{v})) - (d - k - 1)}{\text{wt}(\dot{v}) - k} b_k$$

¹⁷ To avoid having to adopt this convention, we could have used the slightly more standard notation $\sum_{\ell=1}^d (-1)^{v_{j_1} + \dots + v_{j_{\ell}} + \dots + v_{j_d}}$. We opt not to use this notation because it conflicts with our usage of $\hat{\cdot}$ for the discrete Fourier transform.

for each k ($0 \leq k \leq \text{wt}(v) - 1$); the result follows. \square

Corollary 6.5. *For each d ($0 \leq d \leq \text{wt}(v)$), we have $\dim(\mathcal{ZD}_d^0) = 1$.*

7. t -DESIGNS AND EXTREMAL TYPE II CODES

A t -(n, w, λ)-*design* is a (possibly empty)¹⁸ collection D of distinct w -element subsets of $\{1, \dots, n\}$ with the property that $|\{S' \in D : S \subseteq S'\}| = \lambda$ for every $S \subset \{1, \dots, n\}$ with $|S| = t$. This generalizes the notion of a *Steiner system*, which is a t -($n, w, 1$)-design. For example, the codewords of weight 4 in the extended Hamming code form a 3-(8, 4, 1)-design, and the codewords of weight 12 in the extended binary Golay code form a 5-(24, 12, 48)-design. We shall see that these are special cases of behavior common to all extremal Type II codes. When n , w , and λ are undetermined or clear from context, we omit the qualifier “(n, w, λ)” and simply refer to a t -(n, w, λ)-design as a t -*design*. (See [CvL91] for more about t -designs, their uses and their relations with error-correcting codes.)

7.1. An Equivalent Characterization of t -designs. Each $S' \in D$ may be represented by its *indicator vector* (c_1, \dots, c_n) , in which $c_j = 1$ if and only if $j \in S'$. Thus, a t -(n, w, λ)-design D corresponds to a subset of the *Hamming sphere of radius w* ,

$$\sigma_w := \{v \in \mathbb{F}_2^n : \text{wt}(v) = w\}.$$

We henceforth treat this representation of D as completely equivalent to the setwise representation of D , using the relevant terminology interchangeably.

We now introduce the following equivalent characterization of t -designs.

Proposition 7.1. *A set $D \subseteq \sigma_w$ is a t -design if and only if*

$$\sum_{v \in D} Q(v) = 0$$

for all $Q \in \bigcup_{d=1}^t \mathcal{D}_d^0$.

Proposition 7.1 is equivalent to Theorem 7 of Delsarte [Del78]. Our development of \mathcal{D}^0 leads to a new proof of this result, which we present below. In Section 7.2, we apply Proposition 7.1 to prove a special case of the Assmus–Mattson theorem [AM69].

Throughout this section, we write χ_X for the characteristic function of the set X , and recall that \tilde{H} denotes the action of H on $V_1^{\otimes n}$,

$$(7.1) \quad \tilde{H} := \sum \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \cdots \otimes H \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

We begin with a lemma regarding projections of functions $Q \in \mathcal{D}$ to the Hamming sphere σ_w .

Lemma 7.2. *For $Q \in \mathcal{D}$, we have $\chi_{\sigma_w} Q = \pi_{n-2w}(Q)$, where $\pi_{n-2w}(Q)$ is the projection of Q to the $n - 2w$ eigenspace of the action of \tilde{H} on $V_1^{\otimes n}$.*

Proof. This is immediate because the 1- and (-1) -eigenspaces of H are respectively spanned by $\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}\}$ and $\{\begin{pmatrix} 0 \\ 1 \end{pmatrix}\}$. \square

We now demonstrate Proposition 7.1.

¹⁸ Again we allow $D = \emptyset$, which is a t -($n, w, 0$)-design for all t and w . As with spherical designs, for most applications only nonempty D are of interest, but allowing empty designs simplifies the statements of the results relating codes with combinatorial designs.

Proof of Proposition 7.1. We denote by \mathcal{O} the subset of $V_1^{\otimes n}$ consisting of tensor products of t copies of $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ or $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $n - t$ copies of $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$. It is clear that \mathcal{O} spans \mathcal{D}_d for any d ($0 \leq d \leq t$). Now, the set D is a t -design if and only if, for all $R \in \mathcal{O}$,

$$|\sigma_w|(\chi_D, R) = |D|(\chi_{\sigma_w}, R),$$

where $|\cdot|$ is the cardinality function and (\cdot, \cdot) is the inner product. It therefore suffices to show that the set $\{\chi_{\sigma_w} R : R \in \mathcal{O}\}$ is spanned by

$$\bigcup_{d=0}^t \{\chi_{\sigma_w} : Q \in \mathcal{D}_d^0\}.$$

By the second part of Proposition 4.4, any $R \in \mathcal{O}$ may be written in the form

$$R = \sum_{j=0}^t (\tilde{Y}')^j Q_j,$$

with $Q_j \in \bigoplus_{d=0}^{t-j} \mathcal{D}_d^0$. By Lemma 7.2 and the hypothesis, it then only remains to demonstrate that $\pi_{n-2w}((\tilde{Y}')^j Q_j)$ and $\pi_{n-2w}(Q_j)$ are related by a constant factor: for each $j = 0, \dots, t$, we have

$$(7.2) \quad \pi_{n-2w}((\tilde{Y}')^j Q_j) = b \cdot \pi_{n-2w}(Q_j)$$

for some constant b depending on both j and t .

Now, given any $Q \in \mathcal{D}_d^0$, we see by the third part of Proposition 4.4 that the polynomials $(\tilde{Y}')^k Q$ ($0 \leq k \leq n - 2d$) span an irreducible representation of \mathfrak{sl}_2 which is isomorphic to V_{n-2d} . We may regard this representation as $(n - 2d)$ -th homogeneous part of the polynomial algebra $\mathbb{C}[u_0, u_1]$ with generators u_0, u_1 and with actions of X', H', Y' respectively given by

$$(7.3) \quad u'_0 \frac{\partial}{\partial u'_1}, \quad \left(u'_0 \frac{\partial}{\partial u'_0} - u'_1 \frac{\partial}{\partial u'_1} \right), \quad u'_1 \frac{\partial}{\partial u'_0},$$

where $u'_0 = u_0 + u_1$ and $u'_1 = u_0 - u_1$. With this identification, we may take $Q = (u'_0)^{n-2d}$, as

$$Q \in \ker(\tilde{X}' : \mathcal{D}_d^0 \rightarrow \mathcal{D}_{d-1}^0).$$

We now show that $\pi_{n-2w}((\tilde{Y}')^k Q)$ and $\pi_{n-2w}(Q)$ are related by a constant factor for each k ($0 \leq k \leq n - 2d$); the desired expression (7.2) follows. We observe that H acts as

$$(7.4) \quad u_0 \frac{\partial}{\partial u_0} - u_1 \frac{\partial}{\partial u_1}.$$

Therefore, $\pi_{n-2w}(Q) = \pi_{n-2w}((u_0 + u_1)^{n-2d})$ equals $\binom{n-2d}{w-d} u_0^{n-(d+w)} u_1^{w-d}$. To see this, note that $\pi_{n-2w}((u_0 + u_1)^{n-2d}) = \binom{n-2d}{b_1} u_0^{b_0} u_1^{b_1}$ with $b_0 + b_1 = n - 2d$ and $b_0 - b_1 = n - 2w$. (The latter statement follows from the definition of $\pi_{n-2w}(\cdot)$.) Likewise,

$$\pi_{n-2w}((\tilde{Y}')^k Q) = \pi_{n-2w}((\tilde{Y}')^k (u_0 + u_1)^{n-2d})$$

is the $u_0^{n-(d+w)} u_1^{w-d}$ component of $(\tilde{Y}')^k (u_0 + u_1)^{n-2d}$. Since this component is equal to

$$u_0^{n-(d+w)} u_1^{w-d} = \pi_{n-2w}(Q)$$

up to a constant factor, we are done. \square

Remarks. The constant relating $\pi_{n-2w}((\tilde{Y}')^k Q)$ and $\pi_{n-2w}(Q)$ in the proof of Proposition 7.1 was obtained directly from the identification of $\{(\tilde{Y}')^k Q\}_{k=0}^{n-2d}$ with V_{n-2d} . Consequently, this constant is independent of the choice of $Q \in \mathcal{D}_d^0$.

Proposition 7.1 leads to another equivalent characterization of t -designs which makes the analogy between t -designs and spherical t -designs explicit. We have the following corollary, which is equivalent to Theorem 6 of Delsarte [Del78].

Corollary 7.3. *A set $D \subseteq \sigma_w$ is a t -design if and only if*

$$(7.5) \quad \sum_{v \in D} Q(v) = \frac{|D|}{|\sigma_w|} \sum_{v \in \sigma_w} Q(v)$$

for all $Q \in \bigcup_{d=0}^t \mathcal{D}_d$.

Proof. As (7.5) is immediate when Q is constant, the result follows directly from Proposition 7.1 and the second part of Proposition 4.4. \square

Finally, we note that the proof of Proposition 7.1 shows that each $Q \in \mathcal{D}_d^0$ is supported on $\bigcup_{w=d}^{n-d} \sigma_w$. This fact leads to a second proof of Corollary 5.6.

Alternate Proof of Corollary 5.6. As $Q \in \mathcal{D}_d^0$ is supported on $\bigcup_{w=d}^{n-d} \sigma_w$, we know that

$$W_{C,Q}(x, y) = \sum_{w=0}^n \left(\sum_{c \in C_w} Q(c) \right) x^{n-w} y^w = \sum_{w=d}^{n-d} \left(\sum_{c \in C_w} Q(c) \right) x^{n-w} y^w.$$

The result then follows immediately. \square

7.2. The Extremal Type II Code Case of the Assmus–Mattson Theorem. To illustrate the power of Proposition 7.1, we now prove the Assmus–Mattson theorem [AM69] in the important special case of an *extremal Type II code*, that is, a binary linear code C whose minimal (nonzero) weight

$$\min(C) := \min\{\text{wt}(c) : c \in C, c \neq 0\}$$

attains the upper bound $4\lfloor n/24 \rfloor + 4$ derived by Mallows and Sloane [MS73] from Gleason's theorem for Type II codes.

For $n \equiv 0 \pmod{8}$, we define $t(n)$ by

$$(7.6) \quad t(n) := \begin{cases} 5 & n \equiv 0 \pmod{24}, \\ 3 & n \equiv 8 \pmod{24}, \\ 1 & n \equiv 16 \pmod{24}. \end{cases}$$

Theorem 7.4. *If C is an extremal Type II code of length n , then C_w is a t -design for each $t \leq t(n)$ and any w .*

By Proposition 7.1, this theorem follows quickly from the following result, which is slightly more general and is a coding-theoretic analog of the $r > 0$ part of Theorem 2.15.

Proposition 7.5. *If C is an extremal Type II code of length n , then for any w and any choices of $d \in \{1, \dots, t(n)\} \cup \{t(n) + 2\}$ and $Q \in \mathcal{D}_d^0$, we have*

$$\sum_{c \in C_w} Q(c) = 0.$$

Proposition 7.5 was originally proven by Calderbank and Delsarte [CD93]. Here, we demonstrate how Proposition 7.5 follows quickly from Theorem 5.7. This approach is due to Bachoc [Bac99]. Our exposition of this argument slightly expands that of Bachoc [Bac99], which demonstrated only four cases of the result.

Proof of Proposition 7.5. We let $d \in \{1, \dots, t(n)\} \cup \{t(n) + 2\}$ and $Q \in \mathcal{D}_d^0$. Then, we consider the harmonic weight enumerator $W_{C,Q}(x, y)$. By Theorems 5.1 and 5.7, we see that $W_{C,Q}(x, y)/(xy)^d$ is of the form $\xi_{24}^{(\min(C)-d-b_d)/4} \cdot f$, where b_d equals the valuation at y of ψ_d . This factor arises because the valuation at y of $W_{C,Q}(x, y)$ is at least $\min(C)$.

We see that if $W_{C,Q}(x, y)$ is nonzero, then it has degree equal to

$$(7.7) \quad (n \bmod 24) + 4d - 24$$

if $d \equiv 0 \pmod{2}$. Similarly, f has degree

$$(7.8) \quad (n \bmod 24) + 4d - 36$$

if $d \equiv 1 \pmod{2}$. Since (7.7) and (7.8) are always negative for $d \in \{1, \dots, t(n)\} \cup \{t(n) + 2\}$, we must have $f \equiv 0$, whence

$$\sum_{w=0}^n \left(\sum_{c \in C_w} Q(c) \right) x^{n-w} y^w = W_{C,Q}(x, y) \equiv 0. \quad \square$$

We note the following special case of Proposition 7.1 which is relevant to our proofs of configuration results in Section 9.

Corollary 7.6. *If C is an extremal Type II code of length n and $w > 0$, then we have*

$$\sum_{c \in C_w} Q_{t;\psi}(c) = 0$$

for any $t \in \{1, \dots, t(n)\} \cup \{t(n) + 2\}$.

Remarks. As Bachoc [Bac99] illustrates, it is possible to prove the full Assmus–Mattson theorem with a harmonic weight enumerator argument similar to that used in the proof of Proposition 7.5. We have focused on the case of an extremal Type II code because the full force of Corollary 7.6 is required in Section 9.

8. THE KOCH CONDITION ON TYPE II CODES OF LENGTH 24

8.1. Tetrad Systems. For any code C and integer w , define C_w to be the subset of C consisting of codewords of weight w , and define $\mathcal{C}_w(C)$ to be the linear subcode of C generated by C_w . (This notation is analogous to that of Ozeki [Oze86b] for lattices.)

For a doubly even code $C \subset \mathbb{F}_2^n$, the set C_4 is called the *tetrad system* of C . In analogy with the theory of root systems for lattices, the code $\mathcal{C}_4(C)$ generated by C_4 is called the *tetrad subcode* of C , and if $\mathcal{C}_4(C) = C$ then C is called a *tetrad code*. The irreducible tetrad codes are exactly

- the codes d_{2k} ($k \geq 2$), consisting of all words $c \in \mathbb{F}_2^{2k}$ of doubly even weight such that $c_{2j-1} = c_{2j}$ for each $j = 1, 2, \dots, k$;
- the $[7, 3, 4]$ dual Hamming code, called e_7 in this context; and
- the $[8, 4, 4]$ extended Hamming code, here called e_8

(see [Koc87]). We use the names d_{2k} , e_7 , e_8 because the Construction A lattices $L_{d_{2k}}$, L_{e_7} , and L_{e_8} are isomorphic with the root lattices D_{2k} , E_7 , and E_8 respectively.

Analogous to the Coxeter number of an irreducible root system, we define the *tetrad number* $\eta(C)$ of an irreducible tetrad code C of length m to be $|C_4|/m$. A quick computation shows

that each of the m coordinates of C takes the value 1 on exactly $4\eta(C)$ words in C_4 , and that $\eta(d_{2k}) = (k-1)/4$ for each k , while $\eta(e_7) = 1$ and $\eta(e_8) = 7/4$.

8.2. Koch's Tetrad System Condition. Through appeal to the condition of Venkov [Ven80] restricting the possible root systems of Type II lattices of rank 24, Koch [Koc87] obtained a condition on the tetrad systems of Type II codes of length 24. Specifically, he showed the following result.

Proposition 8.1. *If C is a Type II code of length 24, then C has one of the following nine tetrad systems:*

$$(8.1) \quad \emptyset, \quad 6d_4, \quad 4d_6, \quad 3d_8, \quad 2d_{12}, \quad d_{24}, \quad 2e_7 + d_{10}, \quad 3e_8, \quad e_8 + d_{16}.$$

Koch recovered this condition from the Niemeier [Nie73] classification of Type II lattices of rank 24 via Construction A. The condition is also a consequence of the classification of Type II codes of length 24 given by Pless and Sloane [PS75].

8.3. A Purely Coding-Theoretic Proof of Koch's Condition. Here, we present our proof [EK10] of Proposition 8.1 using the theory of harmonic weight enumerators. This argument is closely analogous to that of Venkov [Ven80] for the corresponding criterion on root systems of Type II lattices of rank 24. We thus begin with a coding-theoretic analog of [Ven80, Proposition 1].

Lemma 8.2. *If C is a Type II code of length 24, then*

- *either $C_4 = \emptyset$ or for each j ($1 \leq j \leq 24$) there exists $c \in C_4$ such that $c_j = 1$, and*
- *each irreducible component of $\mathcal{C}_4(C)$ has tetrad number equal to $|C_4|/24$.*

Proof of Lemma 8.2. For each j ($1 \leq j \leq n$), we denote by $Q_{1,j,n}$ the discrete harmonic polynomial defined by

$$(8.2) \quad Q_{1,j,n}(v) := n \cdot (-1)^{v_j} - \sum_{k=1}^n (-1)^{v_k} \in \mathcal{D}_1^0.$$

As in the proof of Proposition 7.5, we see that the harmonic weight enumerator

$$(8.3) \quad W_{C, Q_{1,j,24}}(x, y) = \sum_{w=0}^{24} \left(\sum_{c \in C_w} Q_{1,j,24}(c) \right) x^{24-w} y^w$$

vanishes for each j ($1 \leq j \leq 24$). We then obtain

$$(8.4) \quad \sum_{c \in C_4} (8 - 48c_j) = 0$$

for each j ($1 \leq j \leq 24$), since the left-hand side of (8.4) is the $x^{20}y^4$ coefficient of the discrete Fourier transform of (8.3). Reorganizing (8.4) shows that

$$(8.5) \quad |\{c \in C_4 : c_j = 1\}| = |C_4|/6.$$

The first part of the lemma then follows. In the case that $C_4 \neq \emptyset$, we also obtain from (8.5) that each irreducible component of $\mathcal{C}_4(C)$ has tetrad number $\frac{1}{4}|C_4|/6 = |C_4|/24$. \square

Remark. Since the discrete harmonic polynomial $Q_{1,j,n}$ has degree 1 and is invariant under the coordinate permutations that fix j , it is proportional to the zonal harmonic polynomial $Q_{1;\hat{v}}$ where \hat{v} is the j -th unit vector.

Proof of Proposition 8.1. As noted in Section 8.1, there is at most one tetrad system with tetrad number η for each $\eta \notin \{1, 7/4\}$, while for each $\eta \in \{1, 7/4\}$ there are exactly two tetrad systems with tetrad number η , with $\eta(d_{10}) = \eta(e_7) = 1$ and $\eta(d_{16}) = \eta(e_8) = 7/4$.

Now, Lemma 8.2 implies that if $C_4 \neq \emptyset$, then either C_4 consists of μ copies of the tetrad system d_{2k} for some μ and $k > 1$ such that $\mu \cdot 2k = 24$, or it has one of the following two forms:

- $\delta_{10}d_{10} + \varepsilon_7e_7$, with $\varepsilon_7 > 0$ and $10\delta_{10} + 7\varepsilon_7 = 24$, or
- $\delta_{16}d_{16} + \varepsilon_8e_8$, with $\varepsilon_8 > 0$ and $16\delta_{16} + 8\varepsilon_8 = 24$.

The resulting tetrad systems are precisely the eight nonempty systems listed in (8.1). \square

9. CONFIGURATIONS OF EXTREMAL TYPE II CODES

Let C be an extremal Type II code of length $n = 8, 24, 32, 48, 56, 72$, or 96 . Set $w_0 = \min(C)$, so that $w_0 = 4, 8, 8, 12, 12, 16$, or 20 respectively. We prove that C is generated by C_{w_0} . Our approach uses the harmonic weight enumerator machinery developed in Section 5, following the approach used for lattices in [Ven84], [Oze86a], [Oze86b], and [Kom09a].

First, we present a few brief preliminaries. For any $\hat{v} \in \mathbb{F}_2^n$ and any j ($0 \leq j \leq n$), we denote by $N_j(C; \hat{v})$ the value

$$(9.1) \quad N_j(C; \hat{v}) := |\{c \in C_{w_0}(C) : \text{wt}(c \cap \hat{v}) = j\}|.$$

For $c \in C^\perp$, we must have $N_j(C; c) = 0$ for all odd j .

Lemma 9.1. *If \hat{c} is a minimal-weight representative of the class $[\hat{c}] \in C/C_{w_0}(C)$ and $c \in C_{w_0}$, we have the inequality*

$$\text{wt}(c \cap \hat{c}) \leq \frac{w_0}{2}.$$

Proof. This follows quickly, because if $\text{wt}(c \cap \hat{c}) > w_0/2$, then $[\hat{c}]$ contains a codeword $c + \hat{c}$ of weight

$$\text{wt}(c + \hat{c}) = \text{wt}(c) + \text{wt}(\hat{c}) - 2\text{wt}(c \cap \hat{c}) < \text{wt}(\hat{c}).$$

This contradicts the minimality of \hat{c} in $[\hat{c}]$. \square

We now prove our configuration result for Type II codes of lengths $n = 48$ and 72 . The corresponding results for the remaining values of n are presented in [EK11] and [Kom09b].

Theorem 9.2. *If C is an extremal Type II code of length $n = 48$ or 72 , then*

$$C = C_{w_0}(C).$$

Proof. We consider the equivalence classes of $C/C_{w_0}(C)$ and assume for the sake of contradiction that there is some class $[\hat{c}] \in C/C_{w_0}(C)$ with minimal-weight representative \hat{c} for which $\text{wt}(\hat{c}) = s > w_0$.

As C is self-dual, we have $N_j(C; c) = 0$ for all odd j . Additionally, by Lemma 9.1, we must have $N_{2j'}(C; \hat{c}) = 0$ for $j' > w_0/4$. We now develop a system of equations in the

$$\frac{w_0}{4} + 1$$

variables $N_0(C; \hat{c}), N_2(C; \hat{c}), \dots, N_{w_0/2}(C; \hat{c})$. One such equation is

$$(9.2) \quad N_0(C; \hat{c}) + N_2(C; \hat{c}) + \dots + N_{w_0/2}(C; \hat{c}) = |C_{w_0}|;$$

Corollary 7.6 with $\dot{v} = \dot{c}$ yields $t(n) + 1$ more. This yields a system of

$$t(n) + 2 > \frac{w_0}{4} + 1$$

equations in the variables $N_{2j'}(C; \dot{c})$ ($0 \leq j' \leq w_0/4$).

For $n = 48, 72$, the (extended) determinants of these inhomogeneous systems are

$$(9.3) \quad 2^{26} 3^5 5^2 7^1 11^2 23^2 43^1 47^1 \left(\frac{11s^3 - 396s^2 + 4906s - 20736}{(s-3)(s-2)^2(s-1)^3 s^3} \right),$$

$$(9.4) \quad 2^{42} 3^5 5^2 7^2 11^2 13^1 17^3 23^2 67^2 71^1 \left(\frac{39s^4 - 2600s^3 + 67410s^2 - 800440s + 3650496}{(s-4)(s-3)^2(s-2)^3(s-1)^4 s^4} \right),$$

respectively¹⁹; these determinants must vanish, as they are derived from overdetermined systems. Since equations (9.3) and (9.4) have no integer roots s , we have reached a contradiction. \square

REFERENCES

- [AM69] E. F. Assmus and H. F. Mattson, *New 5-designs*, Journal of Combinatorial Theory **6** (1969), 122–151.
- [Bac99] C. Bachoc, *On harmonic weight enumerators of binary codes*, Designs, Codes and Cryptography **18** (1999), 11–28.
- [Bac01] ———, *Harmonic weight enumerators of non-binary codes and MacWilliams identities*, Codes and Association Schemes (A. Barg and S. Litsyn, eds.), DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 56, American Mathematical Society, 2001, pp. 1–24.
- [CD93] A. R. Calderbank and P. Delsarte, *On error-correcting codes and invariant linear forms*, SIAM Journal on Discrete Mathematics **6** (1993), 1–23.
- [Con69] J. H. Conway, *A characterization of Leech's lattice*, Inventiones Mathematicæ **7** (1969), 137–142.
- [CS99] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed., Springer-Verlag, 1999.
- [CvL91] P. J. Cameron and J. H. van Lint, *Designs, Graphs, Codes and their Links*, Cambridge University Press, 1991, (London Math. Society Student Texts **22**).
- [Del78] Ph. Delsarte, *Hahn polynomials, discrete harmonics, and t -designs*, SIAM Journal on Applied Mathematics **34** (1978), 157–166.
- [Ebe02] W. Ebeling, *Lattices and codes: A course partially based on lectures by F. Hirzebruch*, 2nd ed., Vieweg, 2002.
- [EK10] N. D. Elkies and S. D. Kominers, *On the classification of Type II codes of length 24*, SIAM Journal on Discrete Mathematics **23** (2010), no. 4, 2173–2177.
- [EK11] ———, *Configurations of extremal Type II codes*, in preparation, 2011.
- [Elk00] N. D. Elkies, *Lattices, Linear Codes, and Invariants I, II*, Notices of the American Mathematical Society **47** (2000), 1238–1245 and 1382–1391.
- [Elk11] ———, *On the quotient of an extremal Type II lattice of rank 40, 80, or 120 by the span of its minimal vectors*, in preparation, 2011.
- [Gle71] A. M. Gleason, *Weight polynomials of self-dual codes and the MacWilliams identities*, Actes, Congrès International de Mathématiques (Nice, 1970), vol. 3, Gauthiers-Villars, 1971, pp. 211–215.
- [KAL06] L. F. Klosinski, G. L. Alexanderson, and L. C. Larson, *The Sixty-Sixth William Lowell Putnam Mathematical Competition*, American Mathematical Monthly **113** (2006), 733–743.
- [Kin03] O. D. King, *A mass formula for unimodular lattices with no roots*, Mathematics of Computation **72** (2003), 839–863.
- [Koc87] H. Koch, *Unimodular lattices and self-dual codes*, Proceedings of the International Congress of Mathematicians (Berkeley, Calif., 1986), American Mathematical Society, 1987, pp. 457–465.
- [Kom09a] S. D. Kominers, *Configurations of extremal even unimodular lattices*, International Journal of Number Theory **5** (2009), 457–464.

¹⁹These determinants were computed using the formula of Proposition 6.2. We omit the equations obtained from the zonal spherical harmonic polynomials of the largest degrees when there are more than $\frac{w_0}{4} + 2$ equations obtained by this method.

- [Kom09b] ———, *Weighted generating functions and configuration results for Type II lattices and codes*, Undergraduate Thesis, Harvard University, 2009, http://www.scottkom.com/articles/kominers_thesis.pdf.
- [Kör90] T. W. Körner, *Fourier Analysis*, Cambridge University Press, 1990.
- [Lan75] S. Lang, $SL_2(\mathbb{R})$, Addison-Wesley, 1975.
- [LS71] J. Leech and N. J. A. Sloane, *Sphere packing and error-correcting codes*, Canadian Journal of Mathematics **23** (1971), 718–745.
- [Mac63] F. J. MacWilliams, *A theorem on the distribution of weights in a systematic code*, Bell System Technical Journal **42** (1963), 79–84.
- [MOS75] C. L. Mallows, A. M. Odlyzko, and N. J. A. Sloane, *Upper bounds for modular forms, lattices and codes*, Journal of Algebra **36** (1975), 68–76.
- [MS73] C. L. Mallows and N. J. A. Sloane, *An upper bound for self-dual codes*, Information and Control **22** (1973), 188–200.
- [MS83] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 3rd ed., North-Holland Mathematical Library, vol. 16, North-Holland, 1983.
- [Nie73] H.-V. Niemeier, *Definite quadratische Formen der Dimension 24 und Diskriminante 1*, Journal of Number Theory **5** (1973), 142–178 (German).
- [Ott99] U. Ott, *Local weight enumerators for binary self-dual codes*, Journal of Combinatorial Theory Series A **86** (1999), 362–381.
- [Oze86a] M. Ozeki, *On even unimodular positive definite quadratic lattices of rank 32*, Mathematische Zeitschrift **191** (1986), 283–291.
- [Oze86b] ———, *On the configurations of even unimodular lattices of rank 48*, Archiv der Mathematik **46** (1986), 54–61.
- [PS75] V. Pless and N. J. A. Sloane, *On the classification and enumeration of self-dual codes*, Journal of Combinatorial Theory, Series A **18** (1975), 313–335.
- [Rud76] W. Rudin, *Principles of Mathematical Analysis*, 3rd ed., McGraw-Hill, 1976.
- [Ser73] J.-P. Serre, *A Course in Arithmetic*, Springer-Verlag, 1973.
- [Ser87] ———, *Complex Semisimple Lie Algebras*, Springer-Verlag, 1987.
- [Sie69] C. L. Siegel, *Berechnung von Zetafunktionen an ganzzahligen Stellen*, Nachrichten der Akademie der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse, II **1969** (1969), 87–102 [pages 82–97 in *Gesammelte Abhandlungen IV*, Berlin: Springer 1979].
- [Slo77] N. J. A. Sloane, *Error-Correcting Codes and Invariant Theory: New Applications of a Nineteenth-Century Technique*, American Mathematical Monthly **84** (1977), 82–107.
- [ST54] G. C. Shephard and J. A. Todd, *Finite unitary reflection groups*, Canadian Journal of Mathematics **6** (1954), 274–304.
- [Ven80] B. B. Venkov, *On the classification of integral even unimodular 24-dimensional quadratic forms*, Proceedings of the Steklov Institute of Mathematics **148** (1980), 63–74, \cong [CS99, Chapter 18].
- [Ven84] ———, *Even unimodular Euclidean lattices in dimension 32*, Journal of Mathematical Sciences **26** (1984), 1860–1867.
- [Ven01] ———, *Réseaux et designs sphériques*, Réseaux Euclidiens, Designs Sphériques et Formes Modulaires, Monographies de L'Enseignement Mathématique, vol. 37, Enseignement Mathématique, Genève, 2001, pp. 10–86 (French).

APPENDIX A. PROOF OF GLEASON'S THEOREMS FOR BINARY CODES

Let G_I be the subgroup of $GL_2(\mathbb{C})$ generated by $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $2^{-1/2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and let G_{II} be the subgroup of $GL_2(\mathbb{C})$ generated by $\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ and $2^{-1/2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. We have seen, using (3.7) for the second generator, that if C is a binary code of Type I (respectively Type II) then its weight enumerator W_C is contained in the subring of $\mathbb{C}[x, y]$ invariant under linear substitutions with matrices in G_I (resp. G_{II}). Here we show that the G_I invariants are generated by $x^2 + y^2$ and $\delta_8 := x^2 y^2 (x^2 - y^2)^2$, and the G_{II} invariants are generated by $\varphi_8 = W_{e_8}(x, y) = x^8 + 14x^4 y^4 + y^8$ and $\xi_{24} = x^4 y^4 (x^4 - y^4)^4$. Note that these are consistent with $G_I \subset G_{II}$ because $\varphi_8 = (x^2 + y^2)^4 - 4\delta_8$.

We first show that G_I , and thus also G_{II} , contains the signed permutation subgroup of $GL_2(\mathbb{C})$, which is isomorphic with the eight-element dihedral group and is generated by $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Indeed²⁰ $G_I \ni \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}^2$, and we calculate that $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is the conjugate of $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ by $2^{-1/2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Clearly a polynomial in x, y is invariant under the four matrices $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$ if and only if it is a polynomial in x^2 and y^2 . To be invariant also under $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ it must be a symmetric polynomial in x^2 and y^2 . Thus the invariants under this dihedral group are the polynomials in $x^2 + y^2$ and $x^2 y^2$.

We can already find the G_I -invariant subgroup. Since the involution $2^{-1/2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ fixes $x^2 + y^2$ and takes $x^2 y^2$ to $(x^2 - y^2)^2/4$, it follows that the weight enumerator of a Type I code is a polynomial in $x^2 + y^2$, $x^2 y^2 + (x^2 - y^2)^2/4$, and $x^2 y^2 (x^2 - y^2)^2/4$. Using the identity $x^2 y^2 + (x^2 - y^2)^2/4 = (x^2 + y^2)^2/4$, we dispense with the second of those three generators, and recover Gleason's theorem for self-dual binary codes C (whether of Type I or Type II): the weight enumerator of such a code is a polynomial in $x^2 + y^2$ and δ_8 .

To find instead to G_{II} invariants, we next adjoin the matrix $i \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. We first show that this matrix is contained in the scalar subgroup of G_{II} . We claim that the scalars in G_I are the 8-th roots of unity. Any scalar matrix $\mu \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ has determinant μ^2 , and our generators of G_{II} have determinants i and -1 , so $\mu \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G_{II}$ implies $\mu^8 = 1$. All such μ appear because G_{II} contains

$$(A.1) \quad \left(2^{-1/2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \right)^3 = 2^{-3/2} (2 + 2i) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e^{\pi i/4} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

(The invariance of W_C under $e^{\pi i/4} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ already shows that $8 \mid n$.) In particular G_{II} contains $i \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. This transformation fixes $x^2 y^2$ and takes $x^2 + y^2$ to $-(x^2 + y^2)$. Hence the polynomials invariant under the signed permutation group and $i \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ are precisely the polynomials in $x^2 y^2$ and $(x^2 + y^2)^2$.

Let $Q_1 = (x^2 + y^2)^2$, $Q_2 = -4x^2 y^2$, and $Q_3 = -(Q_1 + Q_2) = -(x^2 - y^2)^2$. We next find elements of G_{II} that permute the Q_j . One is $\varsigma := e^{-3\pi i/4} \cdot 2^{-1/2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, which is a 3-cycle contained in G_{II} by (A.1). We calculate that ς permutes the Q_j cyclically. The other is the diagonal matrix $e^{\pi i/4} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, which takes Q_2 to itself and Q_1, Q_3 to each other. Thus the subring of $\mathbb{C}[x, y]$ invariant under the subgroup of G_{II} generated by signed permutations, $i \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, ς , and $e^{\pi i/4} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ consists of the polynomials in Q_1, Q_2, Q_3 invariant under arbitrary permutations. Since the three Q_j are independent but for the relation $Q_1 + Q_2 + Q_3 = 0$, the invariant subring is generated by their elementary symmetric functions of degrees 2 and 3. We calculate that these are

$$Q_1 Q_2 + Q_3 Q_1 + Q_2 Q_3 = -\varphi_8 \quad \text{and} \quad Q_1 Q_2 Q_3 = 4\psi_2,$$

where $\psi_2 := x^2 y^2 (x^4 - y^4)^2$ is the degree-12 invariant of (5.13). Thus the invariant subring is $\mathbb{C}[\varphi_8, \psi_2]$. Finally the scalar $e^{\pi i/4}$ fixes φ_8 and takes ψ_2 to $-\psi_2$, so the subring of $\mathbb{C}[\varphi_8, \psi_2]$ invariant under $e^{\pi i/4}$ is $\mathbb{C}[\varphi_8, \psi_2^2]$. Since $\psi_2^2 = \xi_{24}$, this proves that any G_{II} -invariant polynomial is contained in $\mathbb{C}[\varphi_8, \xi_{24}]$.

While we proved only that $\mathbb{C}[\varphi_8, \xi_{24}]$ contains the invariant subring $\mathbb{C}[x, y]^{G_{II}}$, we readily conclude that $\mathbb{C}[\varphi_8, \xi_{24}] = \mathbb{C}[x, y]^{G_{II}}$ by verifying that both φ_8 and ξ_{24} are invariant under G_{II} . This can be checked either by direct computation of the action of our generators $2^{-1/2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, or by finding Type II codes C_n of length $n = 8$ and $n = 24$ such that $W_{C_8} = \varphi_8$ and

²⁰ In the coding context we could also show directly that W_C is invariant under $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, that is, that $W_C(x, y) = W_C(y, x)$. Any binary linear code C satisfies $W_C(x, y) = W_C(y, x)$ if and only if C contains the all-1s vector $\mathbf{1}$: in the forward direction, the number of weight n codewords is $W_C(0, 1)$, while $W_C(1, 0) = 1$ always; in the reverse direction, translation by $\mathbf{1}$ gives for each w a bijection between the codewords of weight w and the codewords of weight $n - w$. But we noted already that a self-dual code, whether of Type I or Type II, contains $\mathbf{1}$.

$W_{C_{24}} = \varphi_8^3 + \alpha \xi_{24}$ for some $\alpha \neq 0$. We take for C_8 the extended Hamming code, and for C_{24} the extended Golay code or any of the other indecomposable Type II codes of length 24.

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY
ONE OXFORD STREET
CAMBRIDGE, MA 02138
E-mail address: `elkies@math.harvard.edu`

BECKER FRIEDMAN INSTITUTE FOR RESEARCH IN ECONOMICS
UNIVERSITY OF CHICAGO
1126 EAST 59TH STREET
CHICAGO, IL 60637
E-mail address: `skominers@gmail.com`